ZSCALER AND FORTINET DEPLOYMENT GUIDE

SEPTEMBER 2025, VERSION 1.3

BUSINESS DEVELOPMENT GUIDE

Contents

Terms and Acronyms

The following table defines acronyms used in this deployment guide. When applicable, a Request for Change (RFC) is included in the Definition column for your reference.

Acronym	Definition
CA	Central Authority (Zscaler)
CSV	Comma-Separated Values
CVE	Common Vulnerabilities and Exposures
DLP	Data Loss Prevention
DNS	Domain Name Service
DPD	Dead Peer Detection (RFC 3706)
GRE	Generic Routing Encapsulation (RFC2890)
ICMP	Internet Control Message Protocol
IdP	Identity Provider
IKE	Internet Key Exchange (RFC2409)
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security (RFC2411)
PFS	Perfect Forward Secrecy
PSK	Pre-Shared Key
SaaS	Software as a Service
SLA	Service Level Agreement
SSL	Secure Socket Layer (RFC6101)
TLS	Transport Layer Security
VDI	Virtual Desktop Infrastructure
VPN	Virtual Private Network
XFF	X-Forwarded-For (RFC7239)
ZPC	Zscaler Posture Control (Zscaler)
ZDX	Zscaler Digital Experience (Zscaler)
ZIA	Zscaler Internet Access (Zscaler)
ZPA	Zscaler Private Access (Zscaler)

Trademark Notice

About This Document

The following sections describe the organizations and requirements of this deployment guide.

Zscaler Overview

Zscaler (NASDAQ: ZS) enables the world's leading organizations to securely transform their networks and applications for a mobile and cloud-first world. Its flagship Zscaler Internet Access (ZIA) and Zscaler Private Access (ZPA) services create fast, secure connections between users and applications, regardless of device, location, or network. Zscaler delivers its services 100% in the cloud and offers the simplicity, enhanced security, and improved user experience that traditional appliances or hybrid solutions can't match. Used in more than 185 countries, Zscaler operates a massive, global cloud security platform that protects thousands of enterprises and government agencies from cyberattacks and data loss. To learn more, see **Zscaler's website**.

Fortinet Overview

Fortinet (NASDAQ: FTNT) is a driving force in the evolution of cybersecurity and the convergence of networking and security. Fortinet's mission is to secure people, devices, and data everywhere, and today they deliver cybersecurity everywhere you need it with the largest integrated portfolio of over 50 enterprise-grade products. Well over half a million customers trust Fortinet's solutions, which are among the most deployed, most patented, and most validated in the industry. The Fortinet Training Institute, one of the largest and broadest training programs in the industry, is dedicated to making cybersecurity training and new career opportunities available to everyone. FortiGuard Labs, Fortinet's elite threat intelligence and research organization, develops and uses leading-edge machine learning and AI technologies to provide customers with timely and consistently top-rated protection and actionable threat intelligence. To learn more, refer to **Fortinet's website**.

Audience

This guide is for network administrators, endpoint and IT administrators, and security analysts responsible for deploying, monitoring, and managing enterprise security systems. For additional product and company resources, see:

- **Zscaler Resources**
- **Fortinet Resources**
- **Appendix A: Requesting Zscaler Support**

Software Versions

This document was authored using the latest version of Zscaler software.

Prerequisites

Zscaler Internet Access (ZIA)

- A working instance of ZIA 5.7 or later
- Administrator login credentials to ZIA

Fortinet

- FortiOS 6.2.0 build 0866 (GA) or later
- Administrator login credentials to Fortinet device

Request for Comments

- **For prospects and customers**: Zscaler values reader opinions and experiences. Contact partner-doc-support@zscaler.com to offer feedback or corrections for this guide.
- **For Zscaler employees**: Contact z-bd-sa@zscaler.com to reach the team that validated and authored the integrations in this document.

Zscaler and Fortinet Introduction

Overviews of the Zscaler and Fortinet applications are described in this section.

If you are using this guide to implement a solution at a government agency, some of the content might be different for your deployment. Efforts are made throughout the guide to note where government agencies might need different parameters or input. If you have questions, contact your Zscaler Account team.

ZIA Overview

ZIA is a secure internet and web gateway delivered as a service from the cloud. Think of ZIA as a secure internet on-ramp—just make Zscaler your next hop to the internet via one of the following methods:

- Setting up a tunnel (GRE or IPSec) to the closest Zscaler data center (for offices).
- Forwarding traffic via our lightweight Zscaler Client Connector or PAC file (for mobile employees).

No matter where users connect—a coffee shop in Milan, a hotel in Hong Kong, or a VDI instance in South Korea—they get identical protection. ZIA sits between your users and the internet and inspects every transaction inline across multiple security techniques (even within SSL).

You get full protection from web and internet threats. The Zscaler cloud platform supports Cloud Firewall, IPS, Sandboxing, DLP, and Isolation, allowing you to start with the services you need now and activate others as your needs grow.

ZPA Overview

ZPA is a cloud service that provides secure remote access to internal applications running on a cloud or data center using a zero trust framework. With ZPA, applications are never exposed to the internet, making them completely invisible to unauthorized users. The service enables the applications to connect to users via inside-out connectivity rather than extending the network to them.

ZPA provides a simple, secure, and effective way to access internal applications. Access is based on policies created by the IT administrator within the ZPA Admin Portal and hosted within the Zscaler cloud. On each user device, software called Zscaler Client Connector is installed. Zscaler Client Connector ensures the user's device posture and extends a secure microtunnel out to the Zscaler cloud when a user attempts to access an internal application.

Zscaler UVM Overview

Zscaler Unified Vulnerability Management (UVM) offers a groundbreaking approach to tackling persistent challenges in vulnerability management. Despite decades of focus, traditional vulnerability management tools often fall short due to fragmented data, lack of context, and inefficient prioritization, leaving organizations exposed to threats.

Zscaler UVM redefines the landscape by utilizing its innovative Data Fabric for Security to integrate and enrich data from diverse sources, delivering a holistic and actionable view of an organization's risk posture.

With features like dynamic risk scoring, automated workflows and real-time reporting, Zscaler UVM empowers organizations to prioritize critical vulnerabilities, streamline remediation efforts, and strengthen collaboration across teams. Designed for rapid deployment and measurable impact, UVM helps security leaders transition from reactive, manual processes to a proactive, data-driven strategy, ensuring a more resilient and efficient approach to modern vulnerability management.

Zscaler Resources

The following table contains links to Zscaler resources based on general topic areas.

Name	Definition
ZIA Help Portal	Help articles for ZIA.
ZPA Help Portal	Help articles for ZPA.
Zscaler UVM Help Portal	Help articles for Zscaler UVM.
Zscaler Tools	Troubleshooting, security and analytics, and browser extensions that help Zscaler determine your security needs.
Zscaler Training and Certification	Training designed to help you maximize Zscaler products.
Submit a Zscaler Support Ticket	Zscaler Support portal for submitting requests and issues.

The following table contains links to Zscaler resources for government agencies.

Name	Definition
ZIA Help Portal	Help articles for ZIA.
ZPA Help Portal	Help articles for ZPA.
Zscaler UVM Help Portal	Help articles for Zscaler UVM.
Zscaler Tools	Troubleshooting, security and analytics, and browser extensions that help Zscaler determine your security needs.
Zscaler Training and Certification	Training designed to help you maximize Zscaler products.
Submit a Zscaler Support Ticket	Zscaler Support portal for submitting requests and issues.

FortiGate Overview

FortiGate delivers fast, scalable, and flexible SD-WAN on-premises and in the cloud. Fortinet SD-WAN supports cloud-first, security-sensitive, and global enterprises, as well as the hybrid workforce. The Secure Networking approach uses one operating system and consolidates SD-WAN and application gateway functions.

FortiNDR Overview

Fortinet's SaaS-based FortiNDR Cloud leverages AI and machine learning (ML), behavioral, and human analysis to inspect network traffic to detect malicious behavior early while reducing false positives. FortiNDR Cloud provides unified network traffic visibility across multi-cloud and hybrid environments as well as distributed workforces and constrained, mission-critical environments. FortiNDR Cloud automatically identifies anomalous and malicious behavior, provides risk scores, and shares relevant threat intelligence to assist security teams in prioritizing response efforts.

Lacework FortiCNAPP Overview

Lacework FortiCNAPP is a leading cloud security and compliance platform purpose-built for securing modern, multi-cloud environments. Founded in 2015 and headquartered in California, Lacework was acquired by Fortinet in 2024 to accelerate innovation and enhance its industry-leading cloud-native security offerings as part of a unified cybersecurity platform.

The platform provides continuous, automated visibility and threat detection across AWS, Azure, Google Cloud, Kubernetes, and containerized workloads. Leveraging advanced machine learning and behavioral analytics, Lacework FortiCNAPP proactively identifies anomalies, uncovers vulnerabilities, and mitigates risk—empowering organizations to secure their entire cloud infrastructure without compromising agility.

Designed to integrate seamlessly with existing security stacks, Lacework FortiCNAPP delivers deep, actionable insights that help security teams manage cloud security posture, accelerate threat detection and response, and support DevOps and SaaS environments at scale.

Fortinet Resources

The following table contains links to Fortinet support resources.

Name	Definition
FortiNDR Documentation	Online documentation for FortiNDR.
FortiOS Documentation	Online documentation for FortiOS.
Lacework FortiCNAPP Documentation	Lacework FortiCNAPP documentation and support.
Fortinet Training Institute	Fortinet solution training and certifications.
Fortinet Support	Fortinet solution online support.

Traffic Forwarding with FortiGate

You can configure FortiGate to forward traffic to Zscaler Public Service Edges via GRE or IPSec tunnels.

Configuring GRE and IPSec Tunnels on ZIA

There are three major steps when configuring GRE or IPsec tunnels to ZIA.

1. You must locate which data centers are available to you and the hostname or IP address of the Virtual IP to establish a tunnel towards. To learn more, see **Locating the Hostnames and IP Addresses of Public Service Edges** (government agencies, see **Locating the Hostnames and IP Addresses of Public Service Edges**).
2. You must configure the tunnel itself on the ZIA side. To learn more about configuring a GRE Tunnel and a VPN Credential (for an IPSec tunnel), see:
   - **Configuring GRE Tunnels** (government agencies, see **Configuring GRE Tunnels**)
   - **Adding VPN Credentials** (government agencies, see **Adding VPN Credentials**)
3. You must add the VPN credential to a location. For GRE, the steps are similar, but instead of selecting a VPN Credential, select a Static IP Address. To learn more, see **Configuring Locations** (government agencies, see **Configuring Locations**).

If you have problems with any of these steps, open a ticket with **Zscaler Support** (government agencies, see **Zscaler Support**).

Configuring Fortinet for GRE and IPSec

The following sections explain how to configure Fortinet to use GRE and IPSec tunnels.

Verify Access to FortiOS

To connect to the UI using a web browser, you must configure an interface to allow administrative access over HTTPS or over both HTTPS and HTTP. If you have not changed the admin account password, use the default username, `admin`, and leave the password field blank.

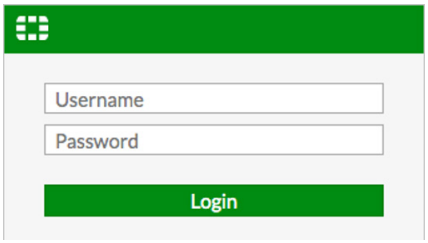

Figure 1. FortiOS Login

FortiGate Dashboard

The dashboard displays various widgets with important system information and allows you to configure some system options. The System Information widget lists information relevant to the FortiGate system, including hostname, serial number, and firmware. The Licenses widget lists the status of various licenses, such as FortiCare Support and IPS.

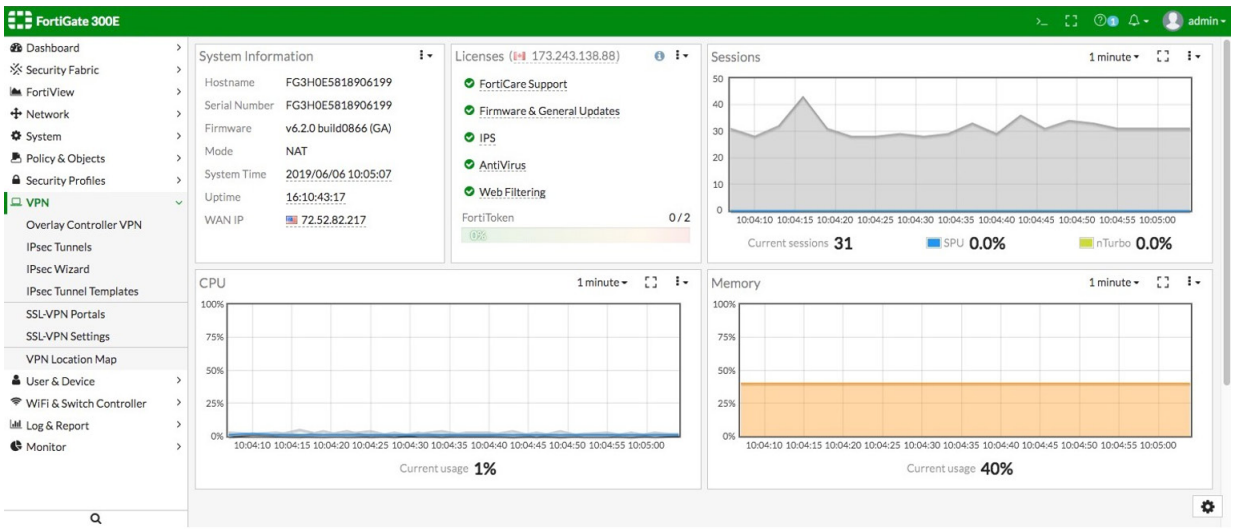

Figure 2. FortiGate Dashboard

Prerequisites to Configuring GRE Tunnels

While you can accomplish most of the tasks to configure your FortiGate using the UI, this configuration guide makes use of advanced features that require the CLI for portions of the configuration.

Create GRE Tunnels

GRE tunnels are configured using the FortiGate CLI. In the following configuration, remote-gw is the IP address of your Zscaler tunnel and local-gw is the IP address of your FortiGate's ISP-facing interface.

This step creates the GRE tunnels and adds them as interfaces to the FortiGate.

```
config system gre-tunnel edit "GRE-SITE1"
  set interface "wan1"
        set remote-gw 199.168.148.131
        set local-gw 72.52.82.217
  next
  edit "GRE-SITE2"
        set interface "wan1"
        set remote-gw 104.129.194.38
        set local-gw 72.52.82.217
  next
end
```

Configure GRE Tunnel Interfaces

This next step configures the newly created FortiGate interfaces. In this config, ip is an address in a /30 subnet provided by Zscaler for the express purpose of GRE tunnel connectivity.

```
config system interface
  edit "GRE-SITE1"
        set ip 172.17.12.129 255.255.255.252
        set allowaccess ping set type tunnel
        set interface "wan1"
  next
  edit "GRE-SITE2"
        set ip 172.17.12.133 255.255.255.252
        set allowaccess ping set type tunnel
        set interface "wan1"
  next
end
```


Performance SLAs

This section explains how to configure Layer-7 Health Checks (aka HTTP Ping).

Prerequisites to Configuring Performance SLAs

If you have not yet done so, configure SD-WAN interfaces as described in **Configuring SD-WAN**. You cannot configure performance SLAs on your FortiGate unless SD-WAN is enabled and at least one interface is marked as an SD-WAN member interface.

Configuring Performance SLAs

You must use the CLI to enable Performance SLA health checks on your new GRE tunnels:

```
config system virtual-wan-link
  config health-check
        edit "Zscaler_VPNTEST"
              set server "gateway.zscalerbeta.net"
              set protocol http
              set http-get "/vpntest"
              set interval 10000
              set failtime 10
              set members 1 2
              configure sla
                    edit 1
                          set latency-threshold 250
                          set jitter-threshold 100
                          set packetloss-threshold 5
                    next
              end
        next
  end
end
```

The rest of this document only uses the HTTP interface.

Configuring IPSec Tunnels

This section only uses the web UI.

IPSec Wizard

To create the VPN, go to **VPN** > **IPsec Wizard** and create a new tunnel using a pre-existing template. Enter a name for the VPN. The tunnel name cannot include any spaces or exceed 13 characters.

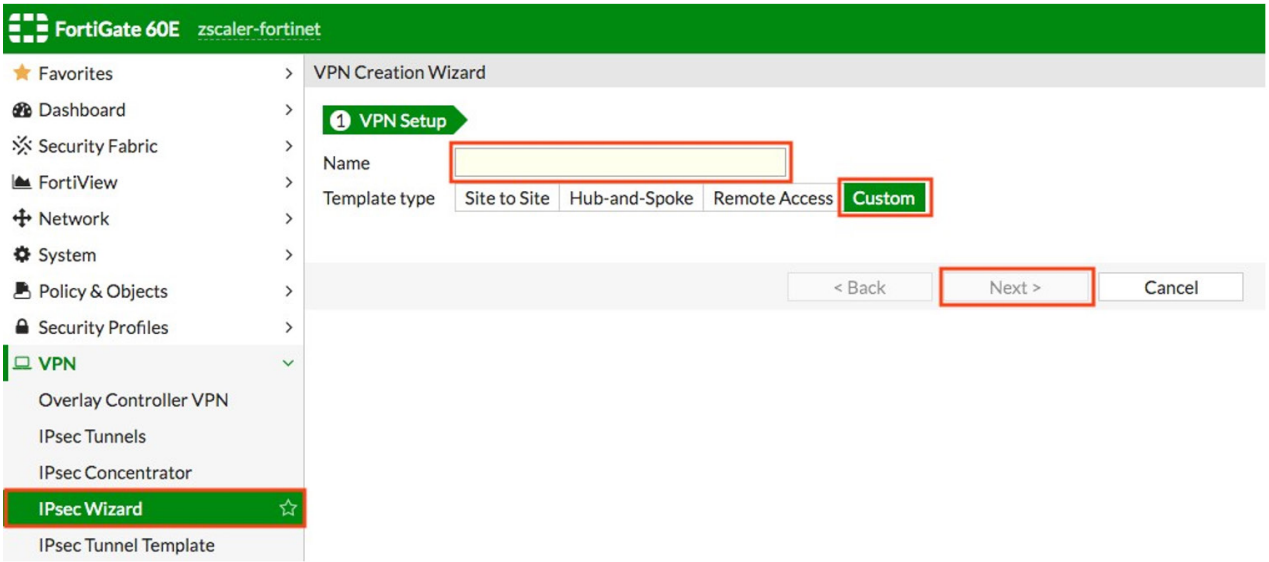

Figure 3. IPSec Wizard—Step 1

Configure IPSec—General

Configure the Network settings, as shown in the following figure. The Dynamic DNS entry is the hostname to the Public Service Edge you want to use.

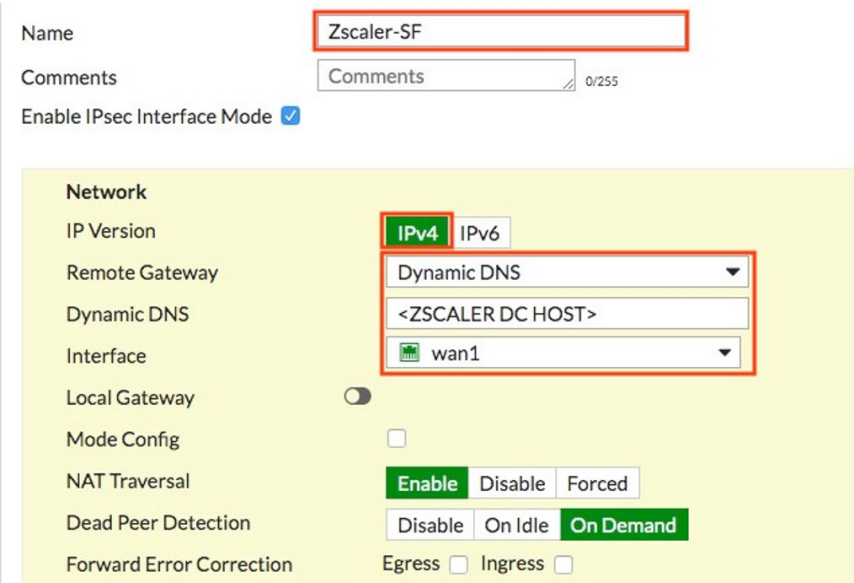

Figure 4. IPSec Wizard—Step 2

Configure IPSec—Phase 1

Configure your settings to match the following figure. The Pre-Shared Key (PSK) is unique per site. The Local ID is the FQDN you configured in the earlier sections.

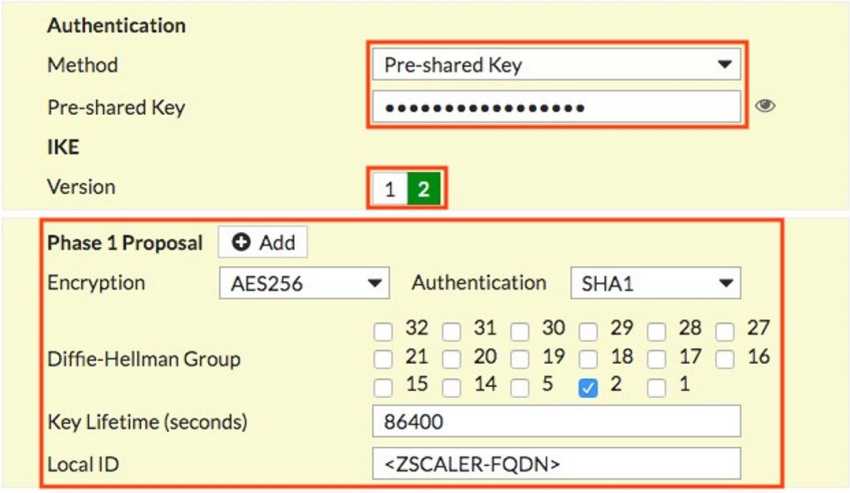

Figure 5. IPSec Wizard—Step 3

Configure IPSec—Phase 2

Configure your settings to match the following figure. When completed, save these settings.

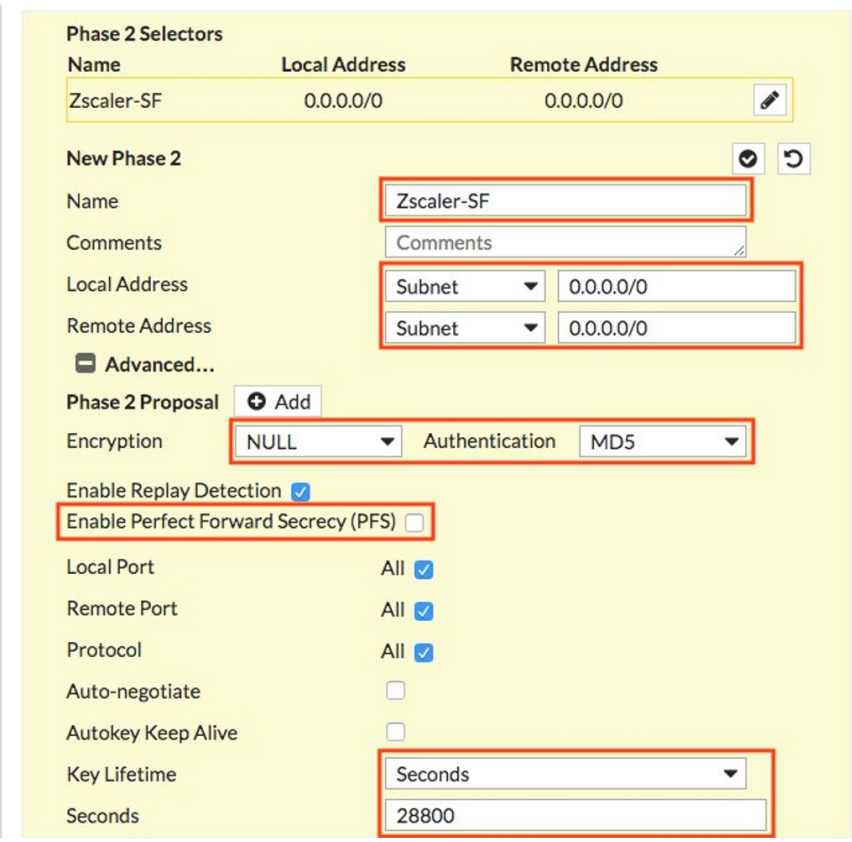

Figure 6. IPSec Wizard—Step 4

Verify IPSec Configuration

After saving your settings, you see your tunnels have a status of Up. If they are not established, recheck your Pre-Shared Key.

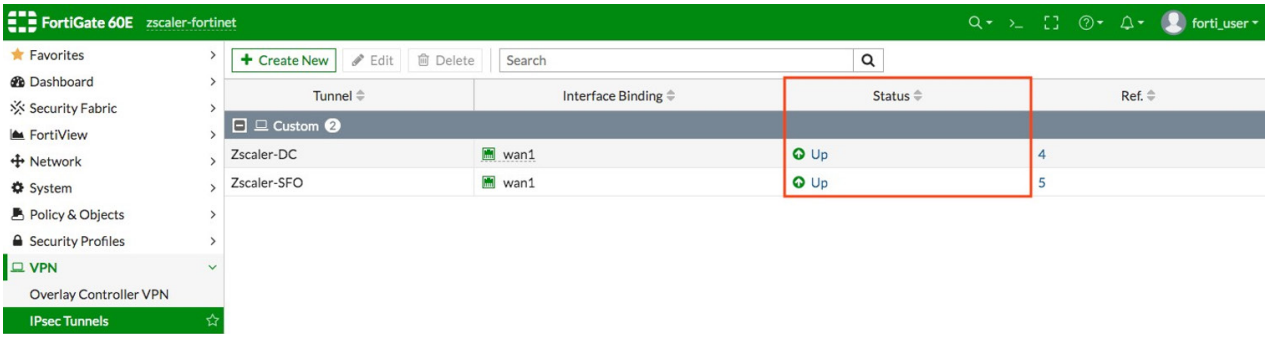

Figure 7. Verify IPSec configuration

Configuring Firewall Policy

The following sections describe how to configure firewall policies.

Create Firewall Policy

When you create a Firewall policy, match the settings with the configuration shown in the following figure. Your Outgoing Interface might have a different name, so adjust this setting to match your internet-facing link.

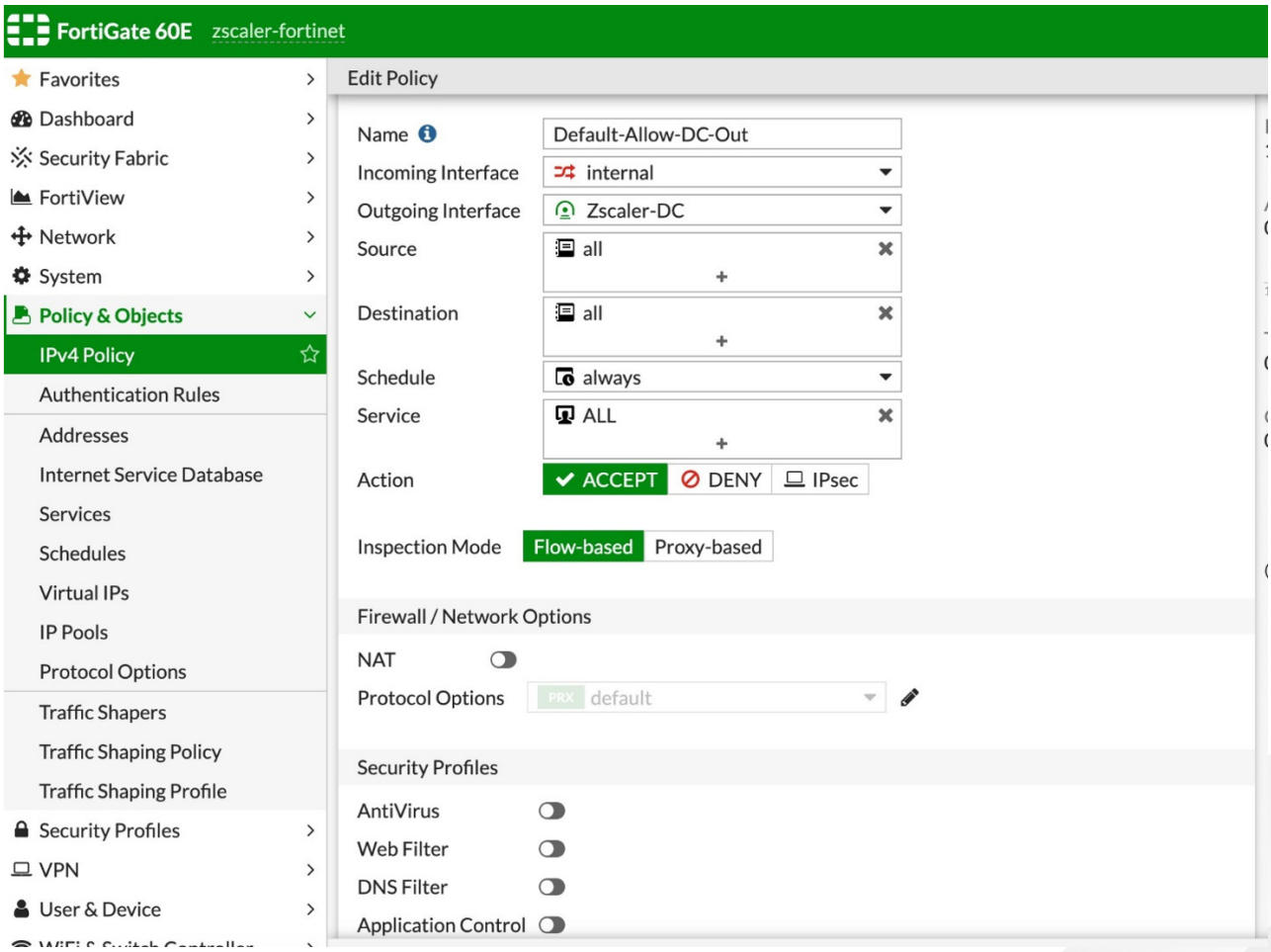

Figure 8. Configure Firewall Policy

Verify Firewall Policies

Duplicate the steps in the following section, as shown next.

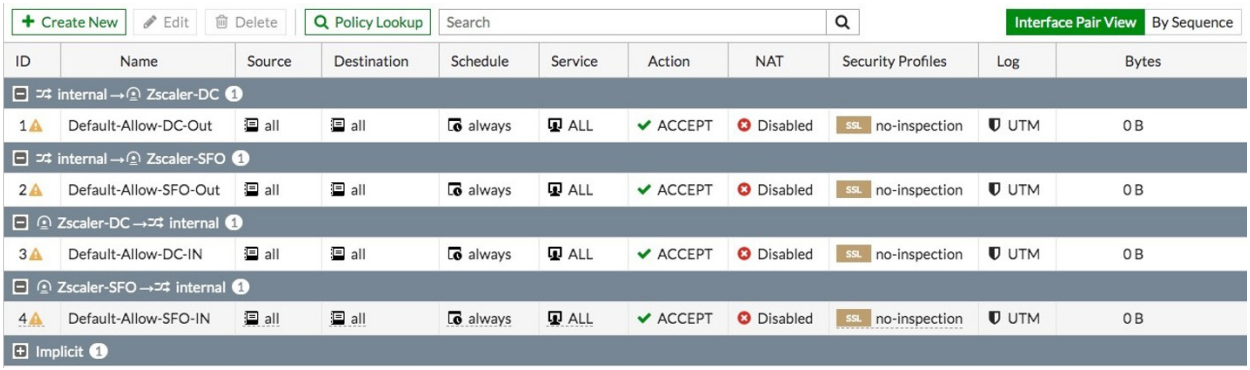

Figure 9. Verify Firewall Policies

Configuring SD-WAN

Configure the primary and secondary ZIA Public Service Edge as a member of the SD-WAN.

Create SD-WAN Member for Primary Public Service Edge

Configure the primary Public Service Edge as a SD-WAN member, with a cost of 5.

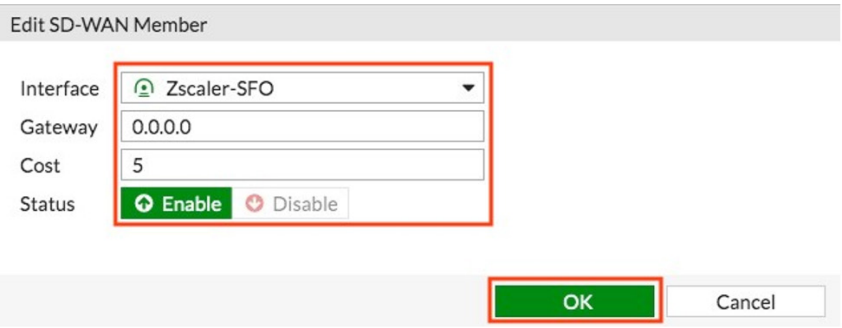

Figure 10. Config SD-WAN for Primary Public Service Edge

Create SD-WAN Member for Secondary Public Service Edge

Configure the primary Public Service Edge as a SD-WAN member, with a cost of 10. Having a higher cost than the prior SD-WAN member determines this SD-WAN member to be secondary (or as a backup).

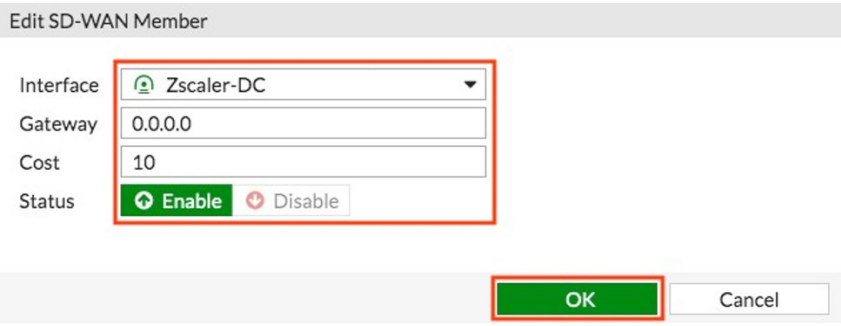

Figure 11. Config SD-WAN for Secondary Public Service Edge

Verify SD-WAN Members

After both SD-WAN members are configured, verify the configuration. Your screen is similar to the following figure.

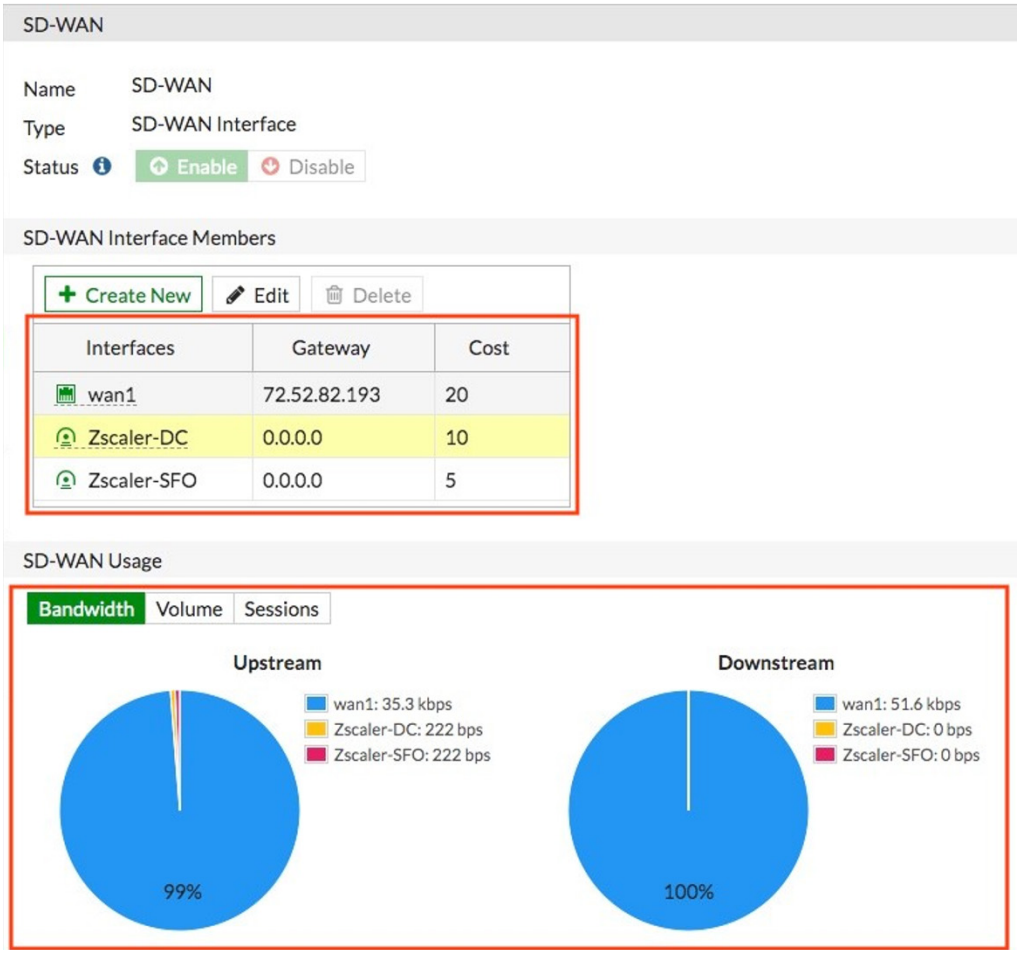

Figure 12. Verify SD-WAN Members

Configuring SD-WAN Rules

This section describes how to configure a SD-WAN rule. This ties the Performance SLA probe to each SD-WAN member for the primary and secondary Public Service Edge.

Create SD-WAN Rule

By using a strategy of Lowest Cost (SLA), this determines which Public Service Edge is the active primary and which Public Service Edge is the standby secondary.

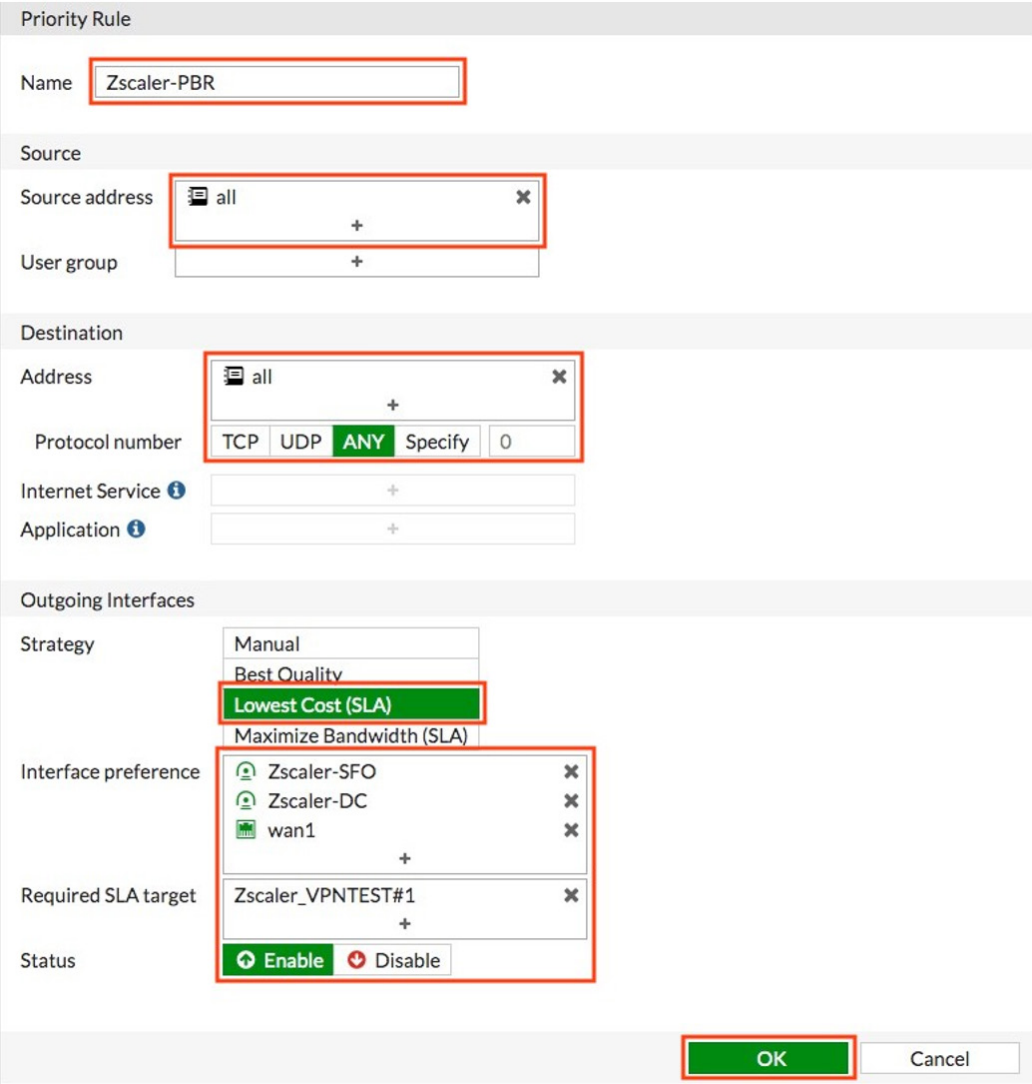

Figure 13. Configure SD-WAN Rule

Verify SD-WAN Rule

After you have configured your SD-WAN rule, verify your configuration. Your screen is similar to the following.

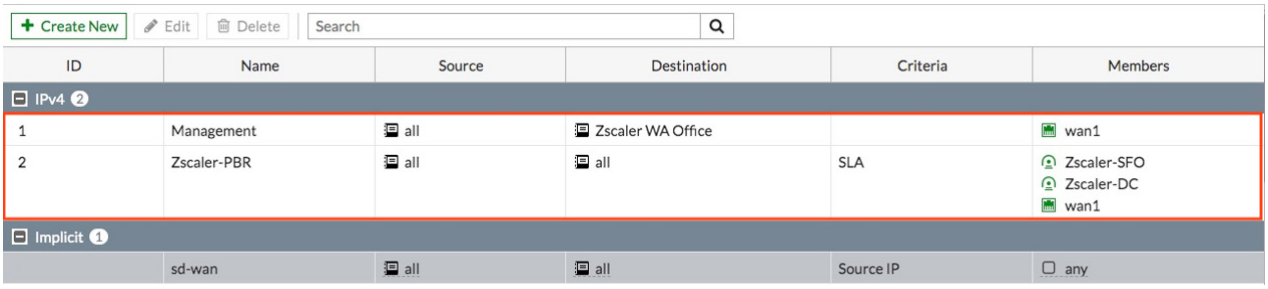

Figure 14. Verify SD-WAN Rule

Verify Configuration with Zscaler Test Page

The following sections describe verifying the configuration with a Zscaler test page.

Request Verification Page

Use the URL https://ip.zscaler.com to confirm if you are transiting ZIA. This is what you see if you are not going through ZIA.

Figure 15. Non-working Example

If you are transiting ZIA, you see the following:

Figure 16. Working Example

FortiNDR Integration

Fortinet NDR solutions combine AI-driven and human analysis to detect and respond to known and unknown network threats. This integration uses logs from ZIA.

This document describes the Zscaler setup needed for log ingestion.

- Zscaler NSS
- Proxy sensor
- NSS feed configuration

Refer to supplemental online documentation for details needed on the Fortinet platform:

- FortiNDR Cloud
- Zscaler setup

Zscaler NSS

Nanolog Streaming Service (NSS) is a Zscaler-provided utility to download logs. Zscaler requires the deployment of virtual machines—one each for web and firewall logs. Customers who have already deployed NSS VMs for external log ingestion can use the same ones for FortiNDR Cloud. If you do not have NSS installed, see the Zscaler help pages or contact Zscaler Support for help.

Proxy Sensor

NSS forwards logs using the syslog protocol. The proxy sensor is designed to receive these logs and upload them to the same destination as FortiNDR Cloud sensors. After ingested, the Zscaler events are mostly treated the same as Zeek events.

The Docker Container must be run from a system that is separate from the NSS log server.

NSS Feed Configuration

After the NSS and proxy sensor instances have been deployed, feeds must be configured to enable logging. See Zscaler's About NSS Feeds (government agencies, see About NSS Feeds) if you need help.

Configuration Issues

It is important that the feeds are configured correctly. If the system is not configured correctly, there is data loss. In the worst case scenario, it can cause problems with the ingest pipeline.

Base Configuration

All feeds share the same base configuration:

Web

1. **Feed Name**: Enter `FortiNDR Cloud—Web`.
2. **NSS Type**: Select **NSS for Web**.
3. **Log Type**: Select **Web Log**.
4. **Feed Output Format**: Copy/paste the following into the **Feed Output Format**.

```
zscaler_log_type=web\ttimestamp=%d{yyyy}-%02d{mth}-%02d{dd}T%02d{hh}:%02d{mm}:%02d{ss}
Z\tzscaler_recordid=%d{recordid}\tzscaler_proto=%s{proto}\tsrc_ip=%s{cip}\tdst_
ip=%s{sip}\tstatus_code=%s{respcode}\tmethod=%s{reqmethod}\tuser_agent=%s{ua}\
treferrer=%s{ereferer}\trequest_length=%d{reqsize}\tresponse_length=%d{resp-
size}\turi=%s{eurl}\tfile_md5=%s{bamd5}\tcontent_type=%s{contenttype}\tclient_ci-
pher=%s{clientsslcipher}\tclient_version=%s{clienttlsversion}\tserver_cipher=%s{s-
rvsslcipher}\tserver_version=%s{srvtlsversion}\tzscaler_username=%s{login}\
tzscaler_hostname=%s{devicehostname}
```

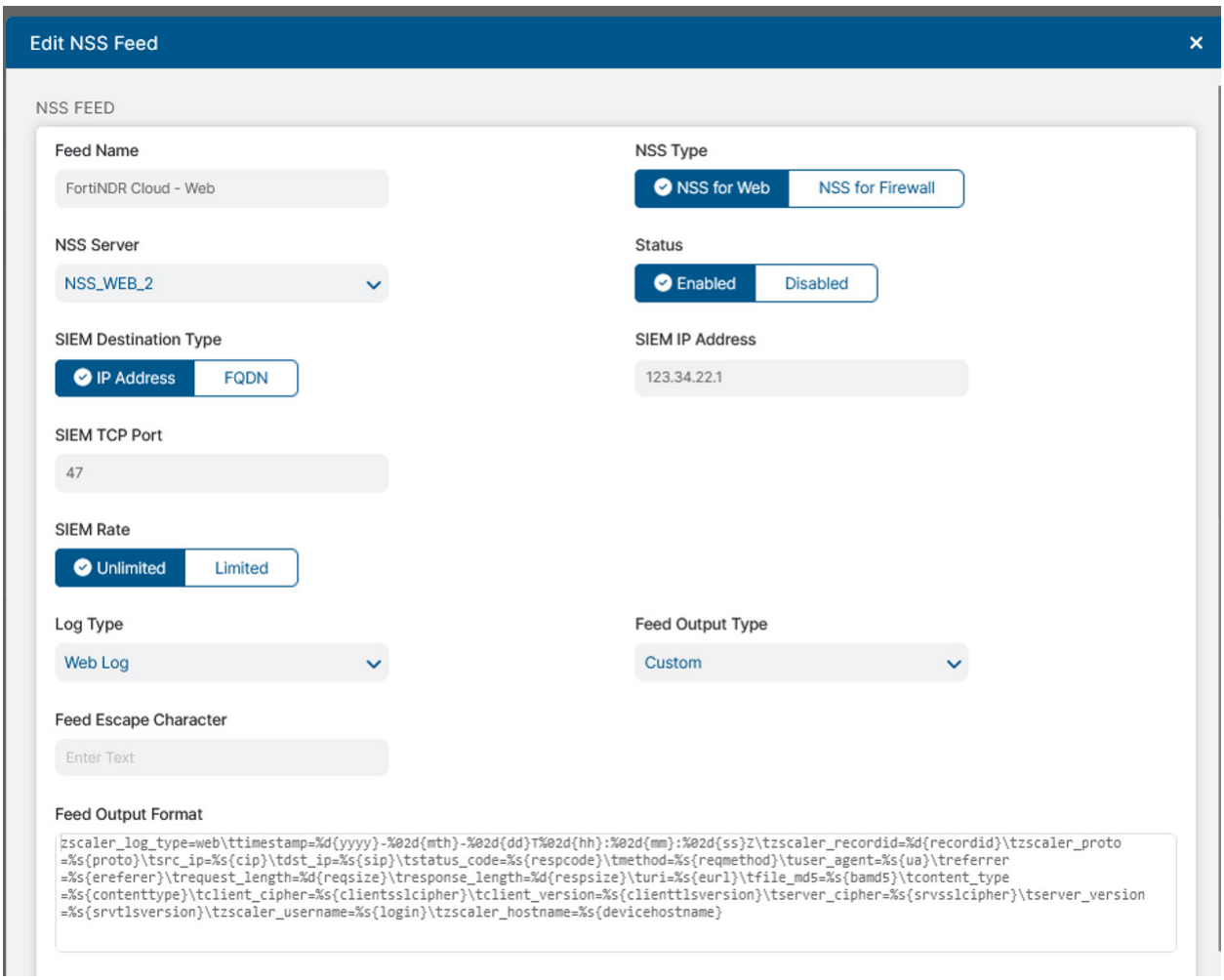

Figure 17. *Web NSS feed*

DNS

1. **Feed Name**: Enter `FortiNDR Cloud—Web`.
2. **NSS Type**: Select **NSS for DNS**.
3. **Log Type**: Select **DNS Log**.
4. **Feed Output Format**: Copy/paste the following into the **Feed Output Format**.

```
zscaler_log_type=dns\ttimestamp=%d{yyyy}-%02d{mth}-%02d{dd}T%02d{hh}:%02d{mm}:%02d{ss}
Z\tzscaler_recordid=%d{recordid}\tsrc_ip=%s{cip}\tdst_ip=%s{sip}\tdst_port=%d{sport}\
tquery=%s{req}\tqtype_name=%s{reqtype}\tresponse=%s{res}\tzscaler_username=%s{login}\
tzscaler_hostname=%s{devicehostname}
```

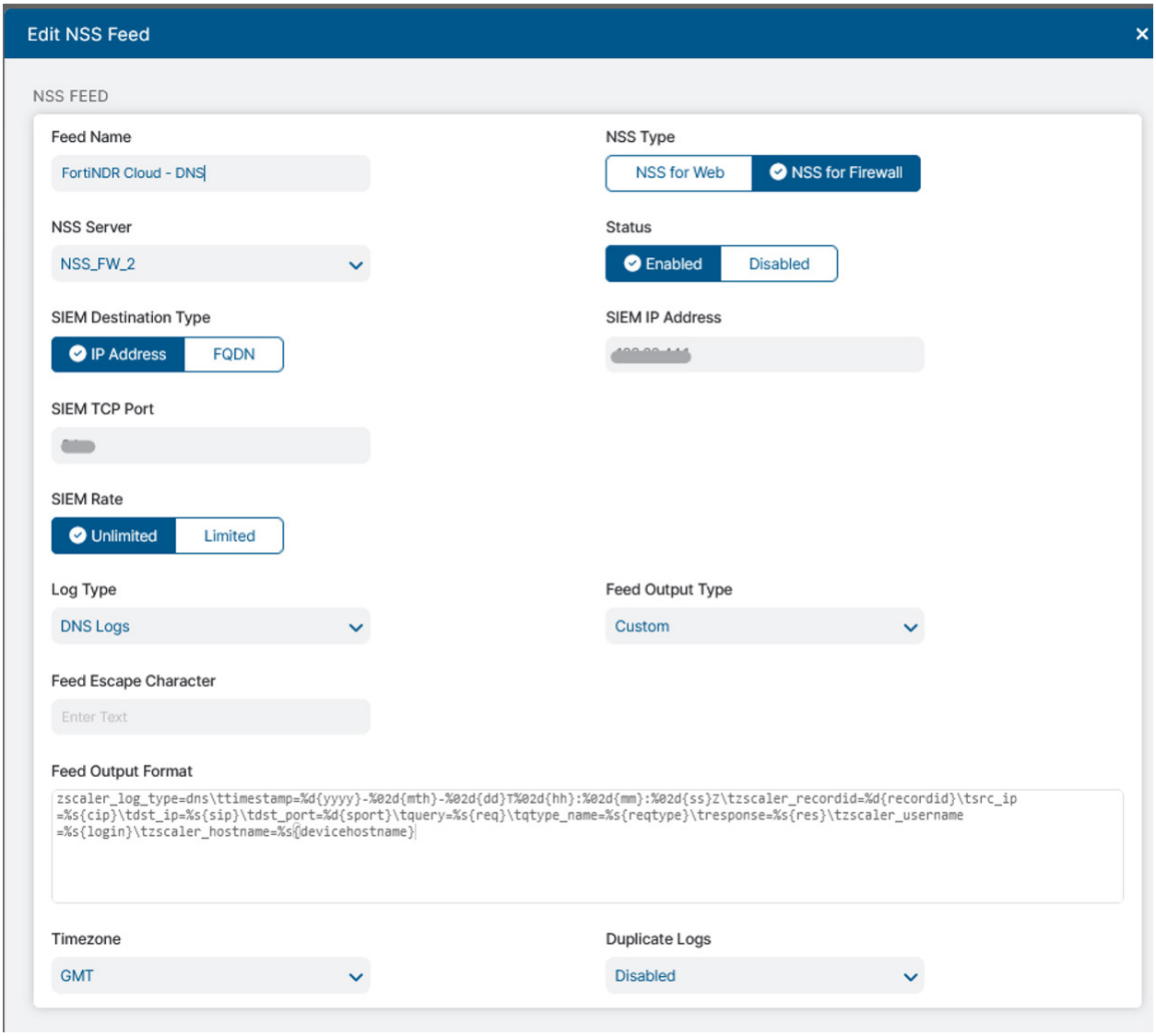

Figure 18. DNS NSS feed

Firewall

1. **Feed Name**: Enter `FortiNDR Cloud—Firewall`.
2. **NSS Type**: Select **NSS for Firewall**.
3. **Log Type**: Select **Firewall Logs**.
4. **Feed Output Format**: Copy/paste the following into the **Feed Output Format**.

```
zscaler_log_type=firewall\ttimestamp=%d{yyyy}-%02d{mth}-%02d{dd}
T%02d{hh}:%02d{mm}:%02d{ss}Z\tzscaler_recordid=%d{recordid}\tsrc_ip=%s{c-
sip}\tsrc_port=%d{csport}\tdst_ip=%s{cdip}\tdst_port=%d{cdport}\tdura-
tion=%d{durationms}\tprotocol=%s{ipproto}\tservice=%s{nwsvc}\trequest_
bytes=%ld{outbytes}\tresponse_bytes=%ld{inbytes}\tzscaler_username=%s{login}\
tzscaler_hostname=%s{devicehostname}
```

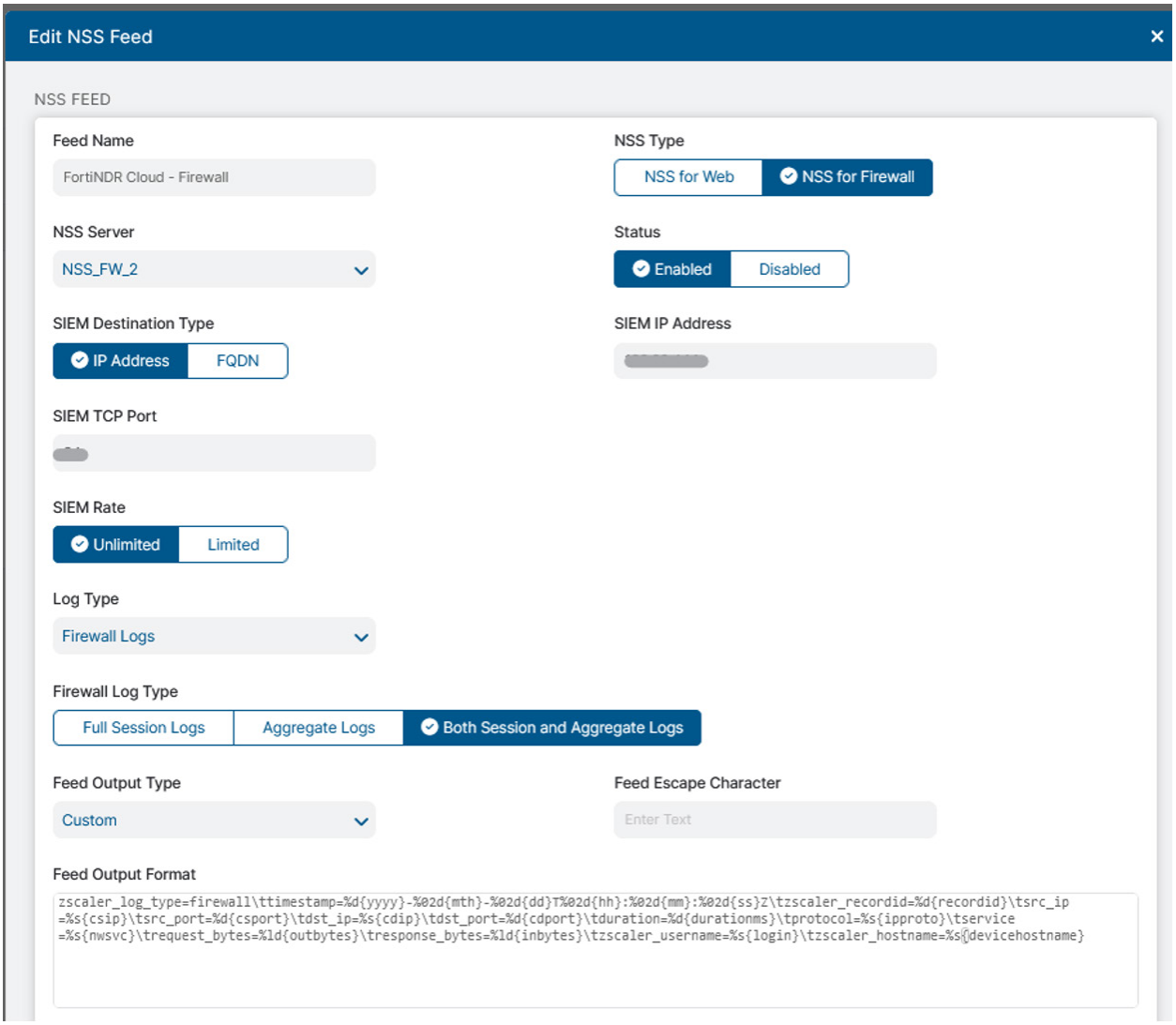

Figure 19. Firewall NSS feed

Cloud NSS

Zscaler Cloud NSS is a managed service from Zscaler. When using Cloud NSS, you do not need to deploy the NSS Virtual Machines. Cloud NSS sends logs to a HTTP endpoint or an S3 bucket. The integration with FortiNDR is through the S3 bucket path. Check with your Zscaler Account team to ensure you have this subscription enabled.

Cloud NSS Setup for S3

The S3 bucket that Zscaler sends logs to is customer-owned. Zscaler accesses it via credentials provided by the customer setup. Ensure that access to the S3 bucket is restricted with proper permissions.

Ensure that you have the following to configure Zscaler Cloud NSS. Contact Fortinet Support to obtain these values.

- AWS Access Id
- AWS Secret Key
- S3 Folder URL

Using S3 requires the correct set of permissions and configuration. To learn more, see the **Zscaler and S3 Deployment Guide, section Zscaler Cloud NSS with Amazon S3**, on setting up S3 to work with Cloud NSS.

Configuring Cloud NSS for Web Logs

1. Log in as an administrator and go to **Administration** > **Nanolog Streaming Service**.

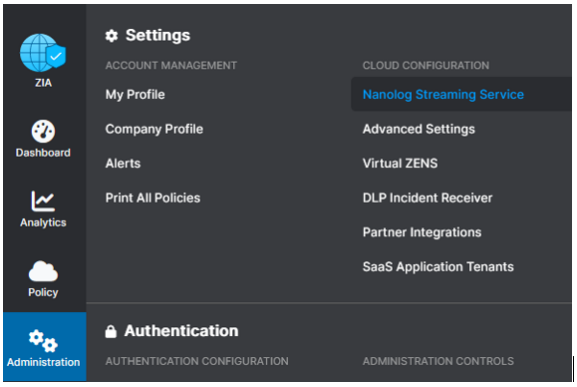

Figure 20. Log in as an administrator

2. Go to **Cloud NSS Feeds** and click **Add Cloud NSS Feed**.

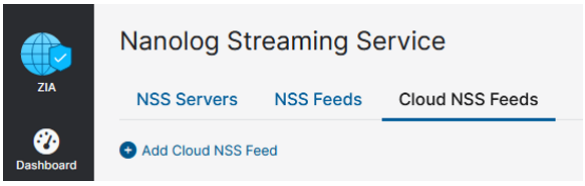

Figure 21. Cloud NSS Feeds

3. In the Add Cloud NSS Feed dialog:
   a. Enter a **Feed Name**.
   b. **NSS Type**: Select **NSS for Web**.
   c. **Status**: Select **Enabled**.
   d. **SIEM Rate**: Select **Unlimited**.
   e. **SIEM Type**: Select **S3**.
   f. Enter information gathered for **S3 Folder URL**, **AWS Access Id**, and **AWS Secret Key**.
   g. Enter a dummy HTTP key and value pair. This is required.
   h. In the **Formatting** section, choose **Web Log**, **Custom type**, and enter `, \"` as the feed escape character.
   i. **Feed Output Format**: Copy/paste the following into the **Feed Output Format**.

```
zscaler_log_type=web\ttimestamp=%d{yyyy}-%02d{mth}-%02d{dd}T%02d{hh}:%02d{mm}:%02d{ss}
Z\tzscaler_recordid=%d{recordid}\tzscaler_proto=%s{proto}\tsrc_ip=%s{cip}\tdst_
ip=%s{sip}\tstatus_code=%s{respcode}\tmethod=%s{reqmethod}\tuser_agent=%s{ua}\
treferrer=%s{ereferer}\trequest_length=%d{reqsize}\tresponse_length=%d{resp-
size}\turi=%s{eurl}\tfile_md5=%s{bamd5}\tcontent_type=%s{contenttype}\tclient_ci-
pher=%s{clientsslcipher}\tclient_version=%s{clienttlsversion}\tserver_cipher=%s{s-
rvsslcipher}\tserver_version=%s{srvtlsversion}\tzscaler_username=%s{login}\
tzscaler_hostname=%s{devicehostname}
```

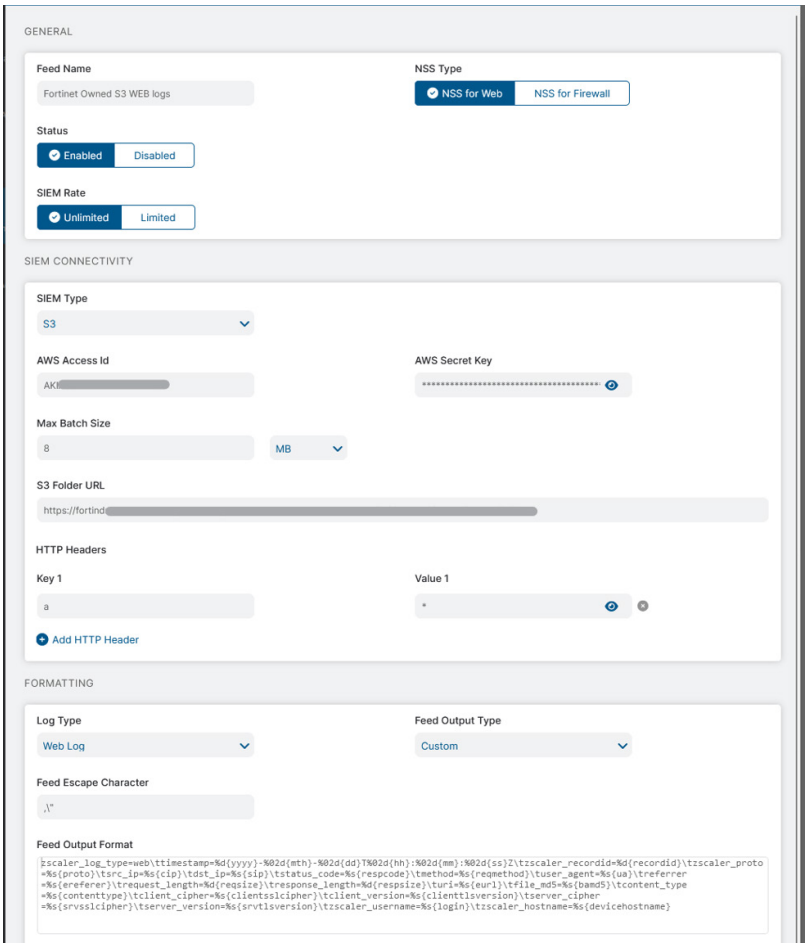

Figure 22. *Web Cloud NSS feed*

Configuring Cloud NSS for Firewall Logs

To configure Firewall logs, follow similar configuration steps for the Web Log with the following exceptions.

1. **NSS Type**: Select **NSS for Firewall**.
2. **Log Type**: Select **Firewall Logs**.
3. **Feed Output Format**: Copy/paste the following into the **Feed Output Format**

```
zscaler_log_type=firewall\ttimestamp=%d{yyyy}-%02d{mth}-%02d{dd}
T%02d{hh}:%02d{mm}:%02d{ss}Z\tzscaler_recordid=%d{recordid}\tsrc_ip=%s{c-
sip}\tsrc_port=%d{csport}\tdst_ip=%s{cdip}\tdst_port=%d{cdport}\tdura-
tion=%d{durationms}\tprotocol=%s{ipproto}\tservice=%s{nwsvc}\trequest_
bytes=%ld{outbytes}\tresponse_bytes=%ld{inbytes}\tzscaler_username=%s{login}\
tzscaler_hostname=%s{devicehostname}
```

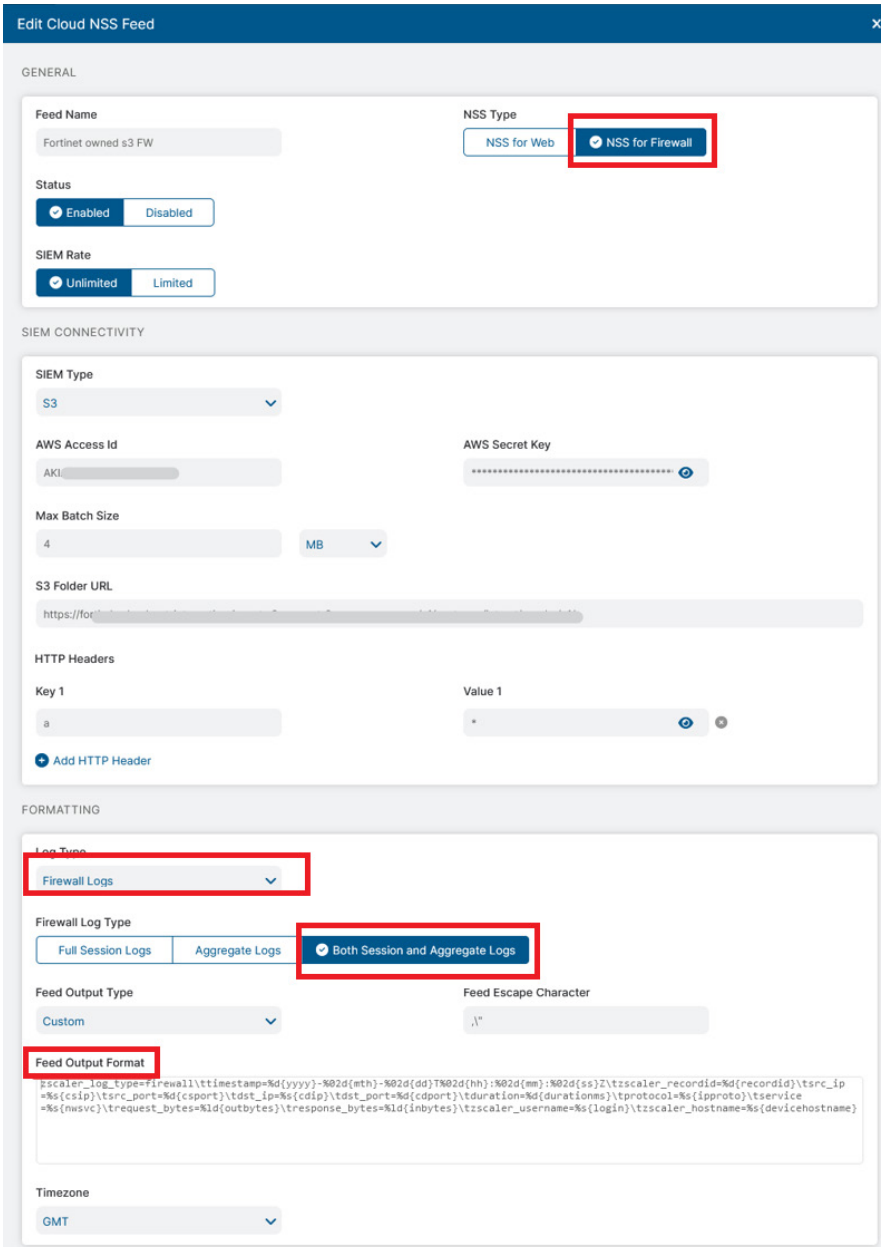

Figure 23. *Firewall Cloud NSS feed*

Configuring Cloud NSS for DNS Logs

To configure DNS logs, follow similar configuration steps for the Web Log with the following exceptions.

1. **NSS Type**: Select **NSS for Firewall**.
2. **Log Type**: Select **DNS Logs**.
3. **Feed Output Format**: Copy/paste the following into the **Feed Output Format**:

```
zscaler_log_type=dns\ttimestamp=%d{yyyy}-%02d{mth}-%02d{dd}T%02d{hh}:%02d{mm}:%02d{ss}
Z\tzscaler_recordid=%d{recordid}\tsrc_ip=%s{cip}\tdst_ip=%s{sip}\tdst_port=%d{sport}\
tquery=%s{req}\tqtype_name=%s{reqtype}\tresponse=%s{res}\tzscaler_username=%s{login}\
tzscaler_hostname=%s{devicehostname}
```

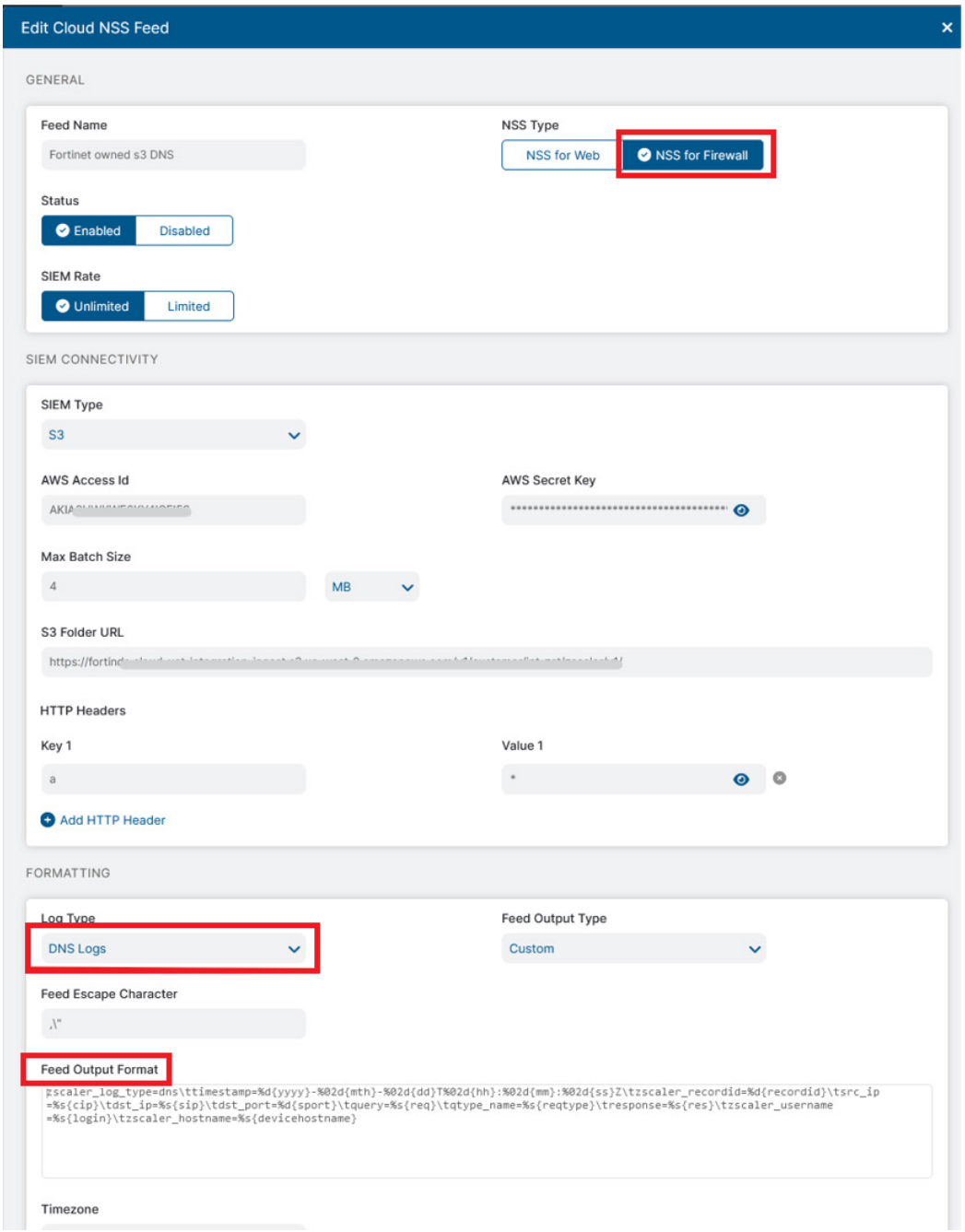

Figure 24. DNS Cloud NSS feed

Contextualizing Risk using Zscaler Unified Vulnerability Management and Lacework FortiCNAPP

Zscaler's Data Fabric and Unified Vulnerability Management (UVM) solution ingests, normalizes, and unifies data across enterprise security and business systems to deliver actionable insights, analytics, and operational efficiencies.

Zscaler UVM offers the following preconfigured Lacework FortiCNAPP connectors:

- Lacework: Retrieves information about the discovered devices, including their attributes and states.
- Lacework Compliance—AWS: Retrieves vulnerability data related to devices, including matched device details.
- Lacework Compliance—GCP: Retrieves vulnerability data related to devices, including matched device details.

Document Prerequisites

To use this document, make sure the following prerequisites are met:

Zscaler UVM:

- An active instance of Zscaler UVM.
- Administrator login credentials to Zscaler UVM.

Lacework FortiCNAPP:

- An active Lacework FortiCNAPP tenant.
- Administrator login credentials to Lacework FortiCNAPP.

ZIA (optional):

- An active instance of ZIA.
- Administrator login credentials to ZIA.

Required Parameters

The source authentication configuration requires the following parameters:

- API Token: Your generated API token.
- Lacework FortiCNAPP Instance: The instance ID of your tenant.

Roles and Permissions

The supplied token must carry at least the following permission:

- Lacework FortiCNAPP Devices: Device > Read
- Lacework FortiCNAPP CVE: Vulnerability > Read

Retrieving the Parameters

The following section describe retrieving the parameters.

Retrieving the API Token

To retrieve your API Token in the FortiCloud Portal, perform the following:

1. Go to **Settings** > **API Keys** > **+ Add New**.

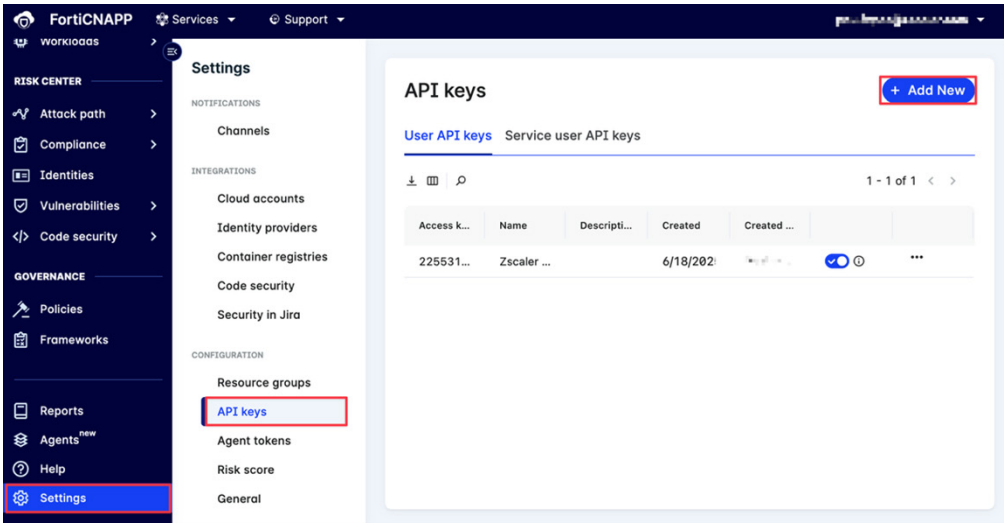

Figure 25. Add new API key

2. Complete the following:
   a. **Name**: Enter a API key name.
   b. **Assign this to a service user**: (Optional) Select this checkbox.
   c. **Service User**: Select the service user to assign this API key to.

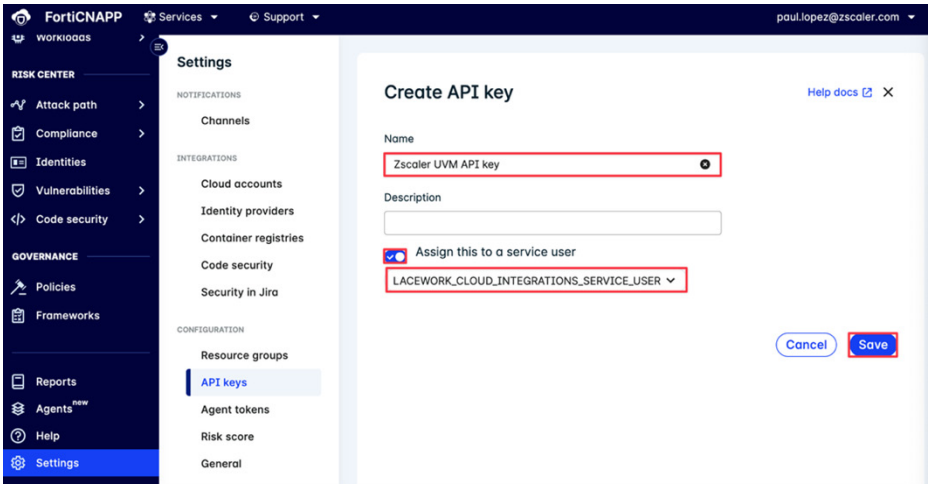

Figure 26. Create API key

   d. Click **Save**.

3. Go to **Settings** > **API keys** > **Service user API keys** and click your API key.

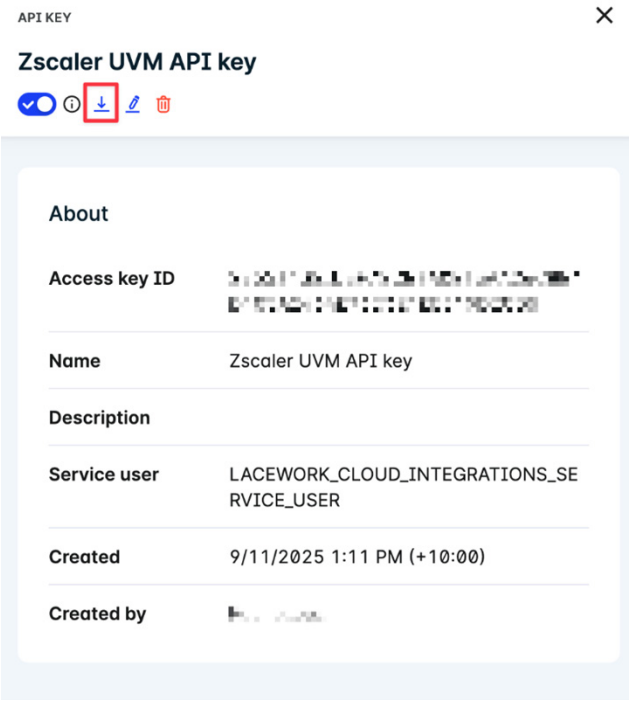

Figure 27. Zscaler UVM API key

4. Download your API key.

Retrieving the Lacework FortiCNAPP Instance

You can find your Lacework FortiCNAPP Instance in your Lacework FortiCNAPP console URL, in the following format:

```
https://<your-instance>.lacework.net
```


Configure the Zscaler UVM Data Connectors

The following sections describe how to configure the Zscaler UVM data connector.

Configure Authentication for the Lacework FortiCNAPP Data Source

1. Log in to the Zscaler UVM Platform.
2. Click **Configure**.

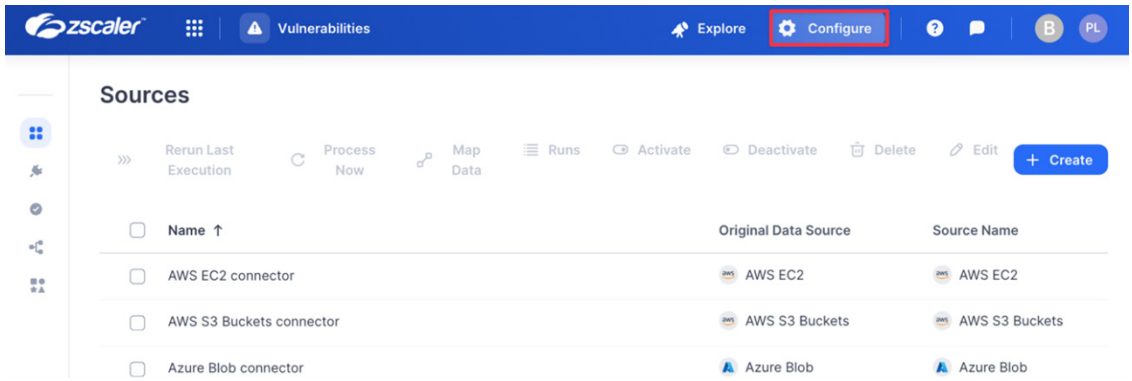

Figure 28. Configure

3. Click **Authentications**.

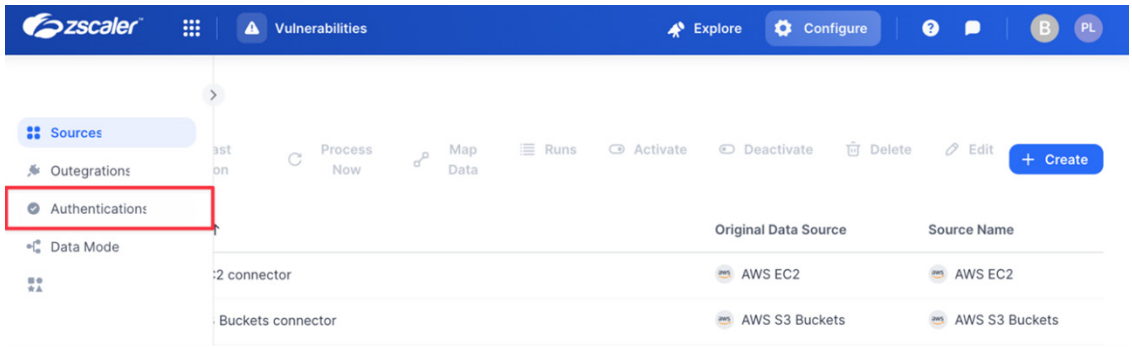

Figure 29. Authentications

4. Click **+ Create**, type `Lacework`, then click **Lacework**.

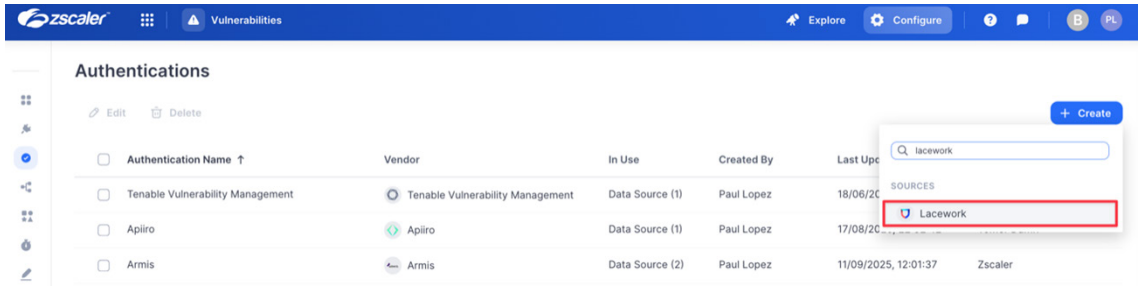

Figure 30. Add Lacework FortiCNAPP authentication

5. Enter the following:
   a. **Name**: Enter an authentication name (i.e., `Lacework`).
   b. **API Key**: Enter the API Key from the previous step.
   c. **API Secret**: Enter the API Secret from the previous step.
   d. **Account Id**: Enter the Account Id from the previous step.

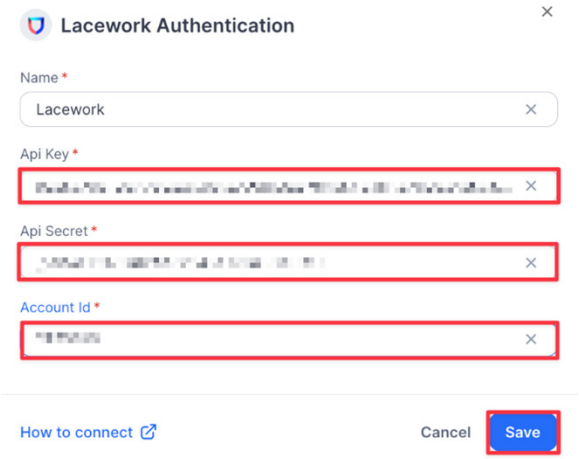

Figure 31. Configure Lacework FortiCNAPP Authentication

   e. Click **Save**.

Configure the Lacework Data Source

1. Log in to the Zscaler UVM Platform.
2. Click **Configure**.

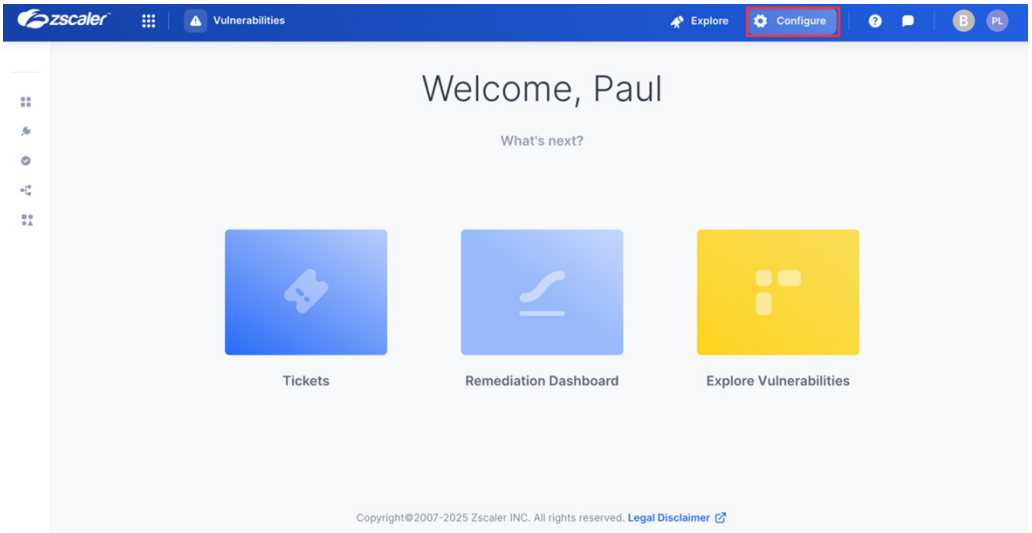

Figure 32. Configure

3. Click **Create**, then search for `Lacework FortiCNAPP Devices`.

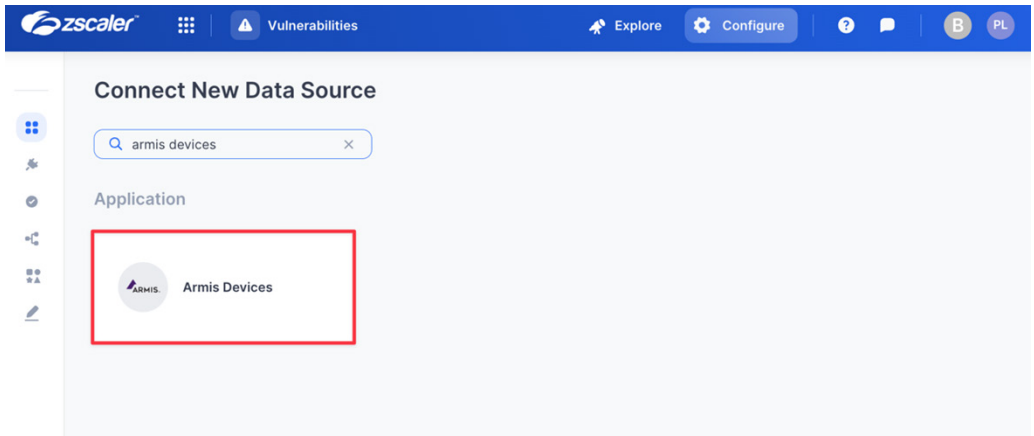

Figure 33. Lacework FortiCNAPP Devices

4. Click the **Lacework FortiCNAPP Secrets** application.
5. On the **Create Lacework FortiCNAPP Secrets Source** page, complete the following:
   a. **Name**: Enter a name for the Data Connector.
   b. **Active**: Toggle the switch to enable the Data Connector.
   c. **Authentication**: Select the authentication source created in the previous step.
   d. **Number of days to fetch**: Enter the number of days to fetch data for.
   e. **Full Refresh Frequency**: Set your desired schedule for extracting all data.
   f. **Remediation Detection Settings**: Select your desired option to determine when findings automatically turn undetected. To learn more, see the **Zscaler documentation**. Automatic remediation detection only applies when data is refreshed fully, not incrementally.
   g. **Suppression Rules**: Define rules and conditions to remove specific data before it enters the Zscaler UVM system. To learn more, see the **Zscaler documentation**.
6. Click **Test**. If the API key and region have been entered correctly, the system responds with **Test Passed**.

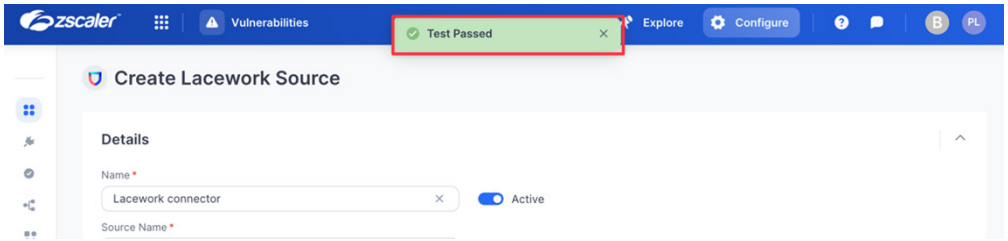

Figure 34. Test Passed

7. Click **Save**.

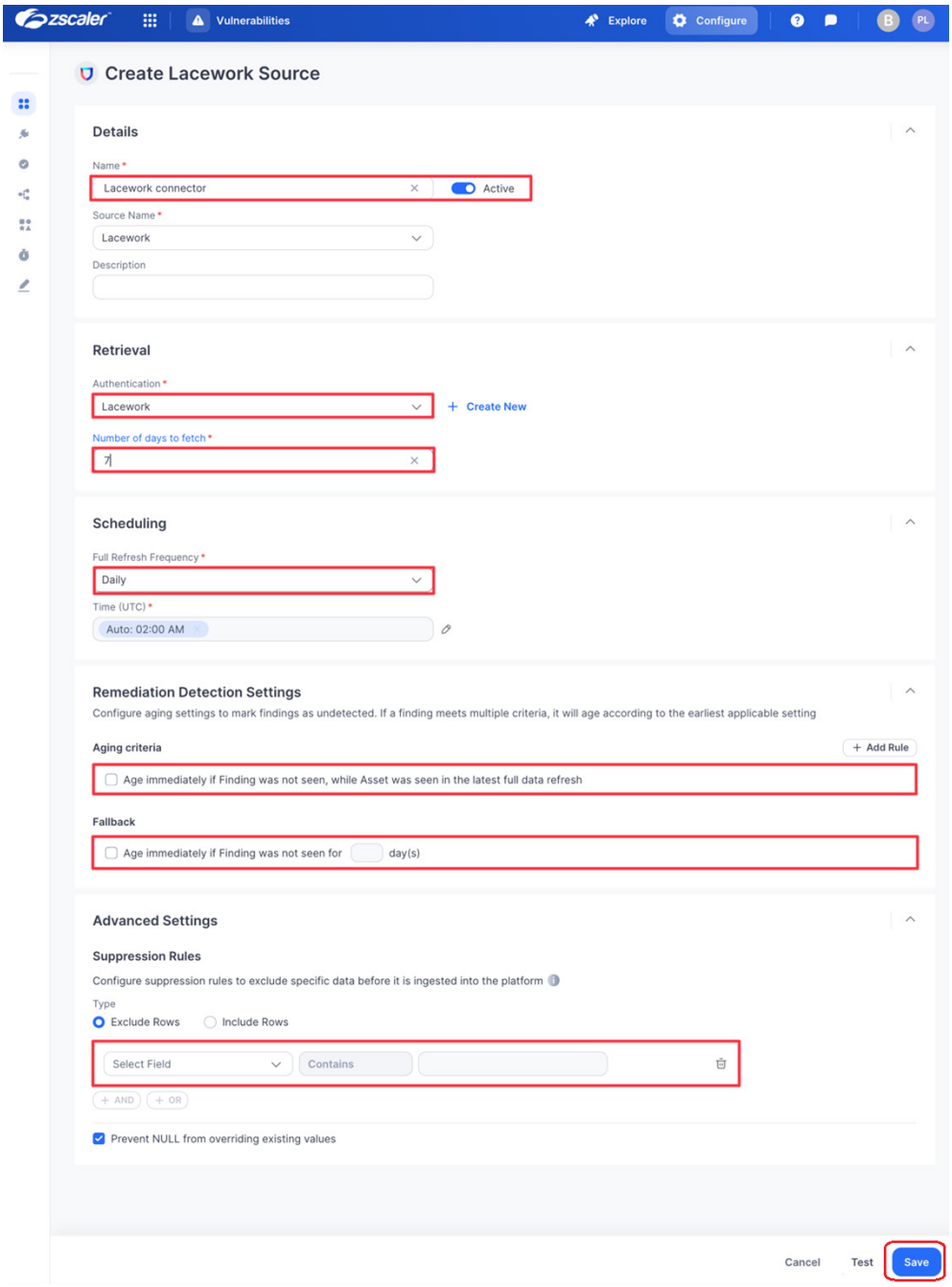

Figure 35. Create Lacework Source

Configure the Lacework Compliance—AWS Data Source

1. Log in to the Zscaler UVM Platform.
2. Click **Configure**.

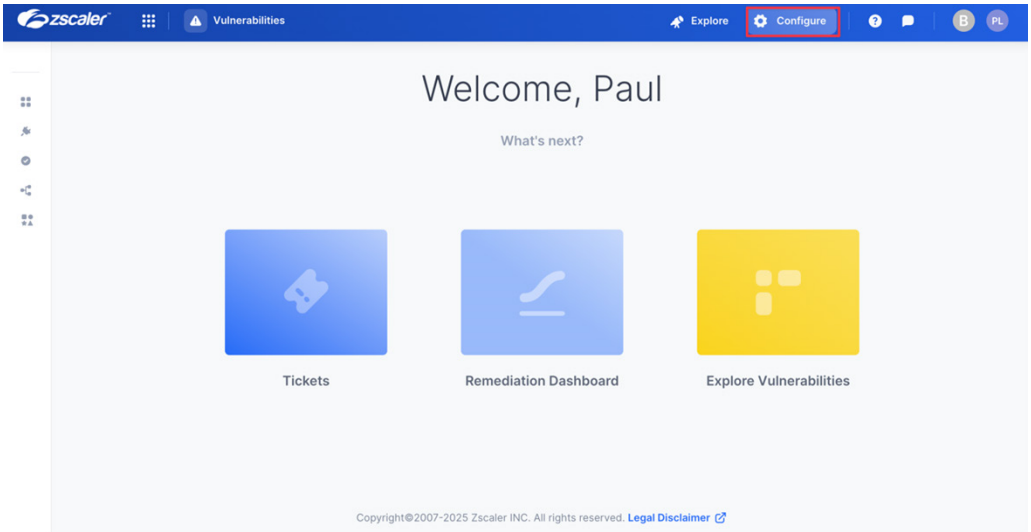

Figure 36. Configure

3. Click **Create**, then search for `Lacework Compliance—AWS`.

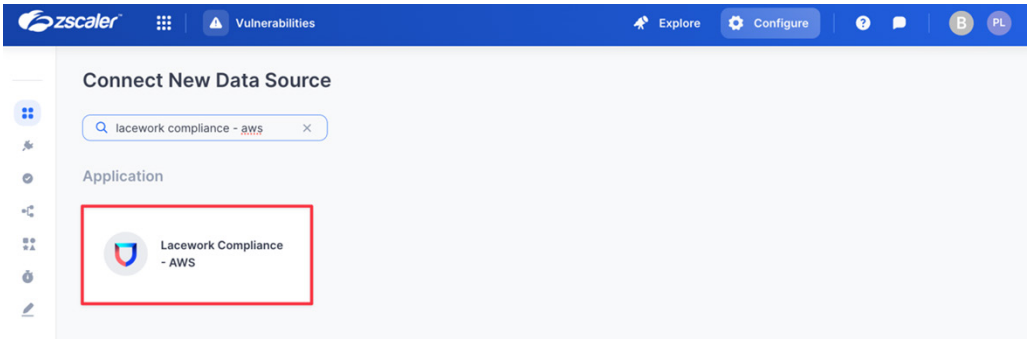

Figure 37. Lacework Compliance—AWS

4. Click the **Lacework Compliance—AWS** application.
5. On the **Create Lacework Compliance—AWS Source** page, complete the following:
   a. **Name**: Enter a name for the Data Connector.
   b. **Active**: Toggle the switch to enable the Data Connector.
   c. **Authentication**: Select the authentication source created in the previous step.
   d. **Number of days to fetch**: Enter the number of days to fetch data for.
   e. **Full Refresh Frequency**: Set your desired schedule for extracting all data.
   f. **Remediation Detection Settings**: Select your desired option to determine when findings automatically turn undetected. To learn more, see the Zscaler documentation. Automatic remediation detection only applies when data is refreshed fully, not incrementally.
   g. **Suppression Rules**: Define rules and conditions to remove specific data before it enters the Zscaler UVM system. To learn more, see the Zscaler documentation.

6. Click **Test**. If the API key and region have been entered correctly, the system responds with **Test Passed**.

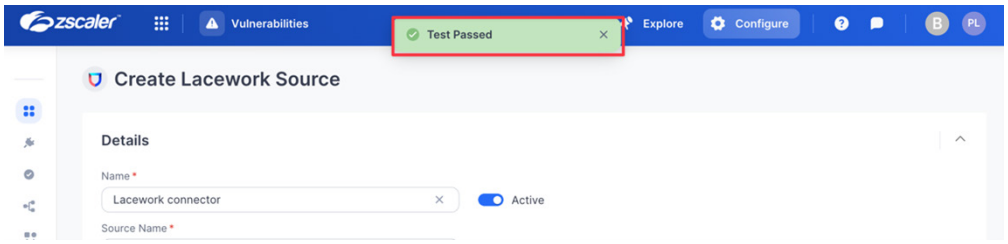

Figure 38. Test Passed

7. Click **Save**.

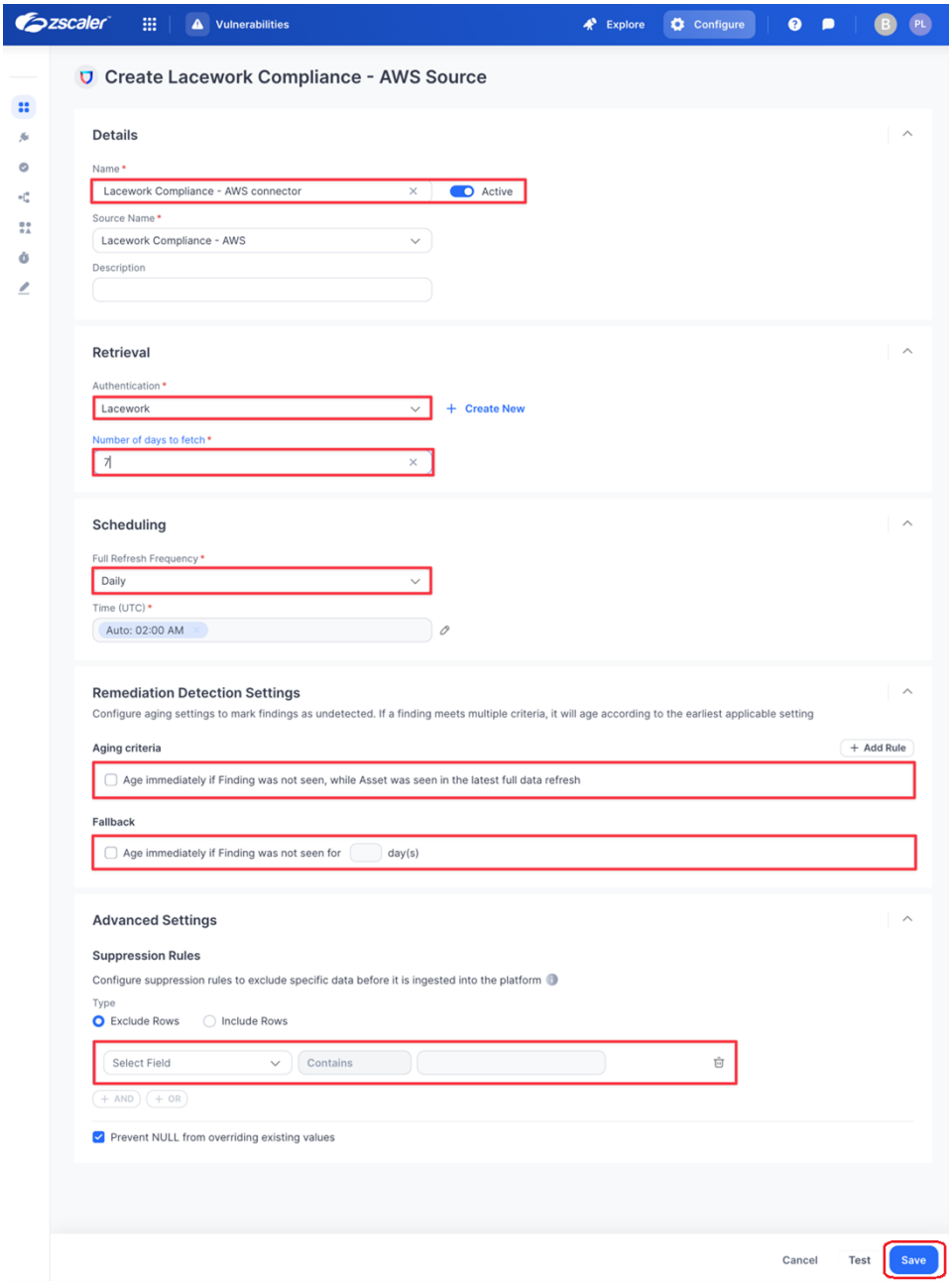

Figure 39. Create Lacework Compliance—AWS Source

Configure the Lacework Compliance—GCP Data Source

1. Log in to the Zscaler UVM Platform.
2. Click **Configure**.

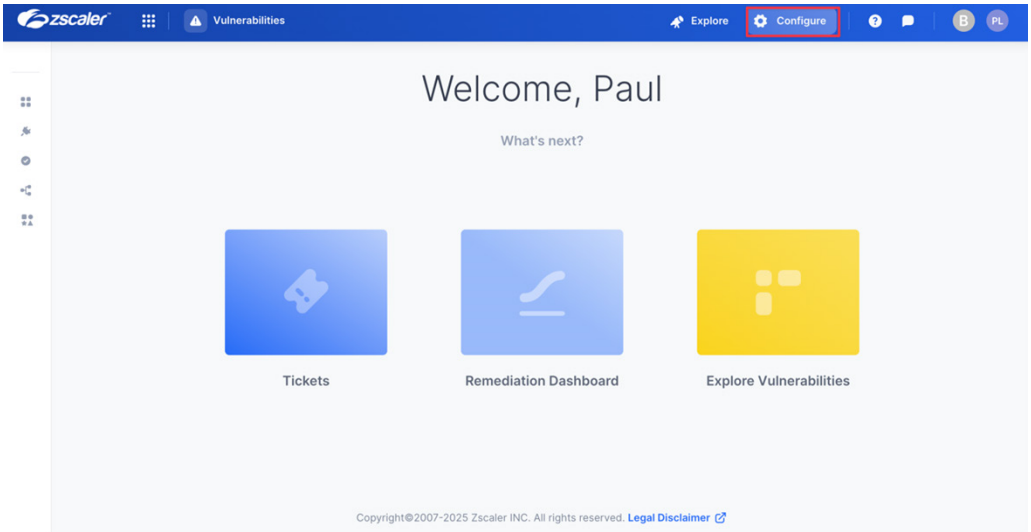

Figure 40. Configure

3. Click **Create**, then search for `Lacework Compliance—GCP`.

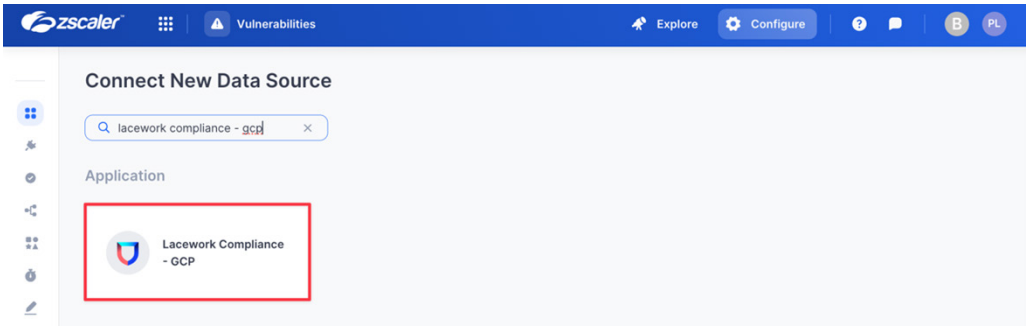

Figure 41. Lacework Compliance—GCP

4. Click the **Lacework Compliance—GCP** application.
5. On the **Create Lacework Compliance—GCP Source** page, complete the following
   a. **Name**: Enter a name for the Data Connector.
   b. **Active**: Toggle the switch to enable the Data Connector.
   c. **Authentication**: Select the authentication source created in the previous step.
   d. **Number of days to fetch**: Enter the number of days to fetch data for.
   e. **Full Refresh Frequency**: Set your desired schedule for extracting all data.
   f. **Remediation Detection Settings**: Select your desired option to determine when findings automatically turn undetected. To learn more, see the **Zscaler documentation**. Automatic remediation detection only applies when data is refreshed fully, not incrementally.
   g. **Suppression Rules**: Define rules and conditions to remove specific data before it enters the Zscaler UVM system. To learn more, see the **Zscaler documentation**.

6. Click **Test**. If the API key and region have been entered correctly, the system responds with **Test Passed**.

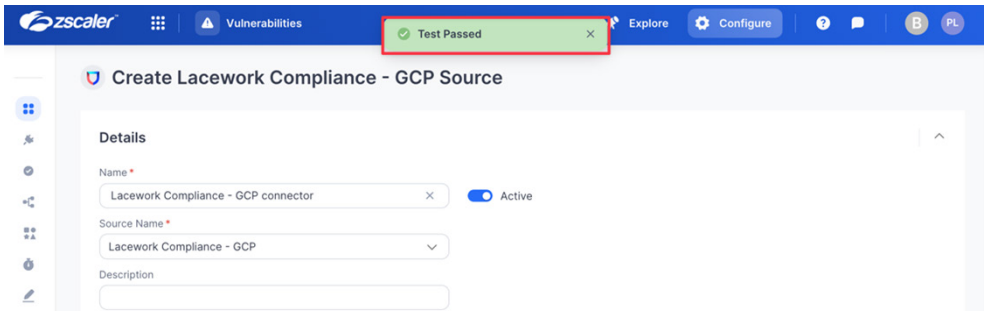

Figure 42. Create Lacework Compliance—GCP Source

7. Click **Save**.

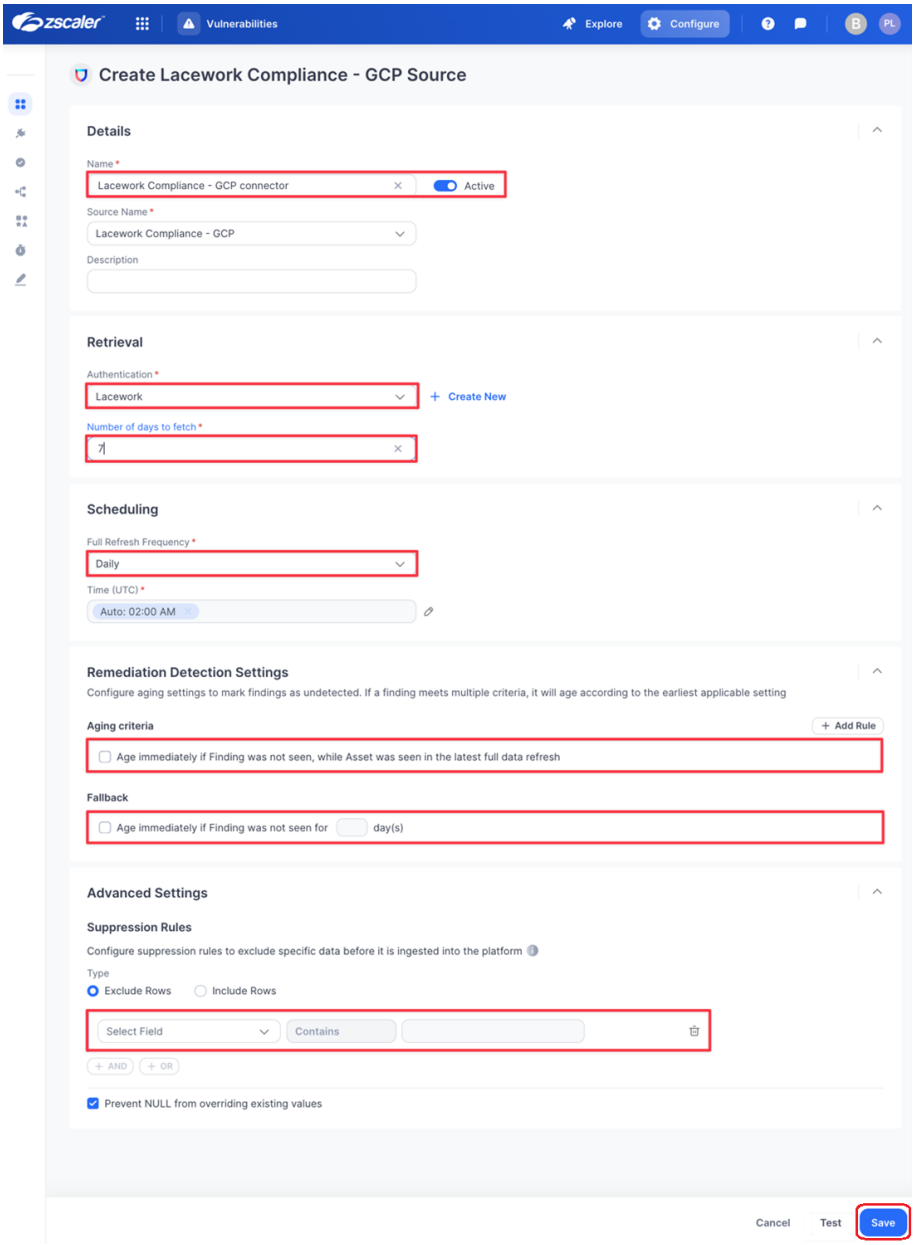

Figure 43. Create Lacework Compliance—GCP Source

Review and Adjust Risk Scoring

(Optional) Zscaler UVM automatically maps ingested data to its default Data Model, allowing you to start analysis immediately. However, your data source might contain extra context that can further refine risk prioritization.

After ingested data has been normalized and mapped to the Data Model, Zscaler UVM can evaluate risk.

The following example illustrates how to map the severity attribute from the Lacework Compliance—GCP data source as a Risk Factor for a Finding when assessing risk.

Map the Lacework Compliance—GCP Data Source

To map the Finding/Key field to the id ingested data field:

1. Select **Configure** > **Lacework Compliance—GCP connector** > **Map Data**.

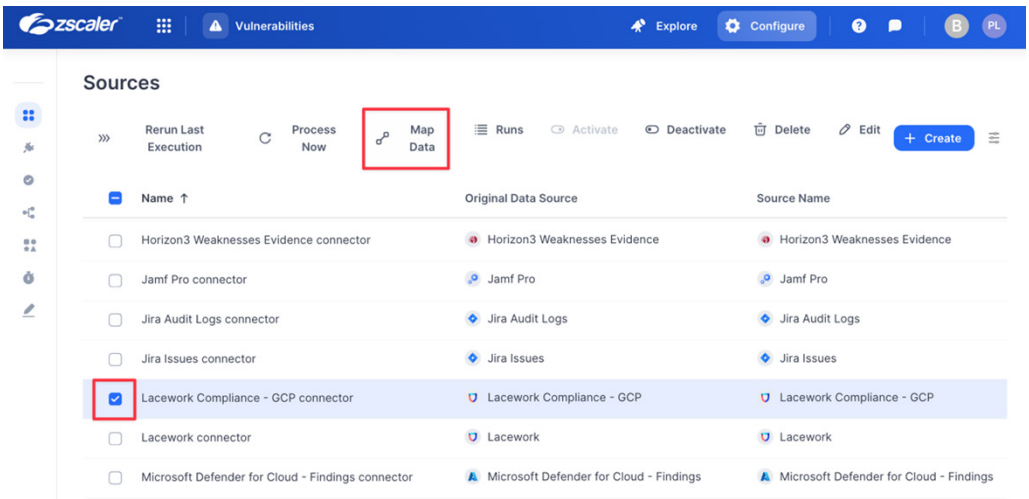

Figure 44. Sources

2. Map the **Finding/Key** entity to the resouce field by:
   a. On the right side, under **Finding**, drag **Key** to the **Create New Connection** element.
   b. On the left side, click the resource field.

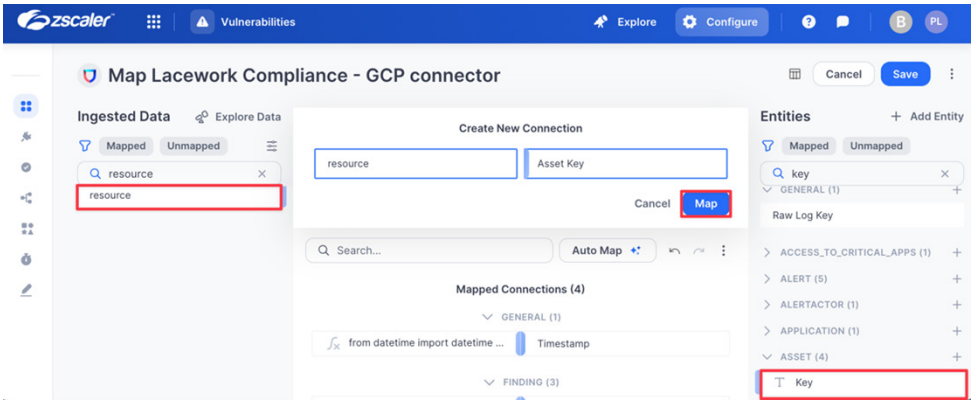

Figure 45. Map Lacework Compliance—GCP connector

   c. Click **Map**.

3. Map the **Finding/Description** entity to the **reason** field by:
   a. On the right side, under **Finding**, drag **Description** to the **Create New Connection** element.
   b. On the left side, click the **reason** field.

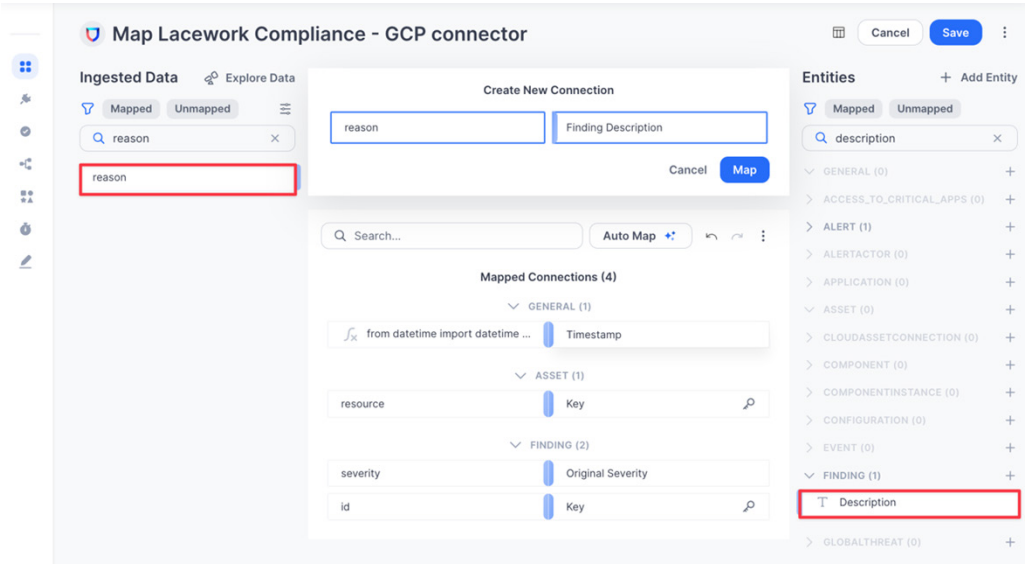

Figure 46. Reason

   c. Click **Map**.

4. Map the **Finding/Original Severity** entity to the severity by:
   a. On the right side, under **Finding**, drag **Original Severity** to the **Create New Connection** element.
   b. On the left side, click the **severity** field.

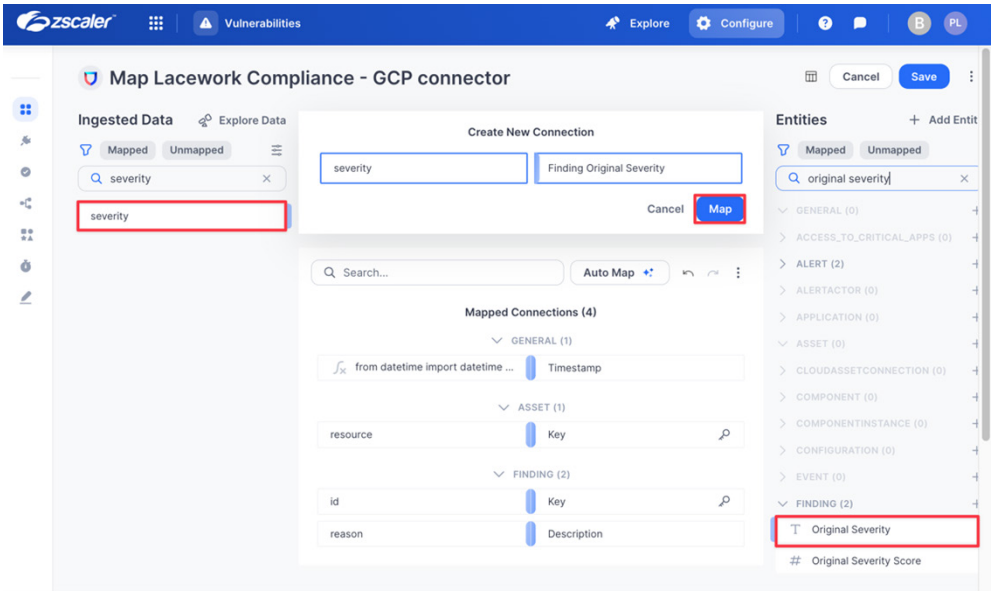

Figure 47. Severity

   c. Click **Map**.

5. Map the **Finding/Key** entity to the id by:
   a. On the right side, under **Finding**, drag **Key** to the **Create New Connection** element.
   b. On the left side, click the **id** field.

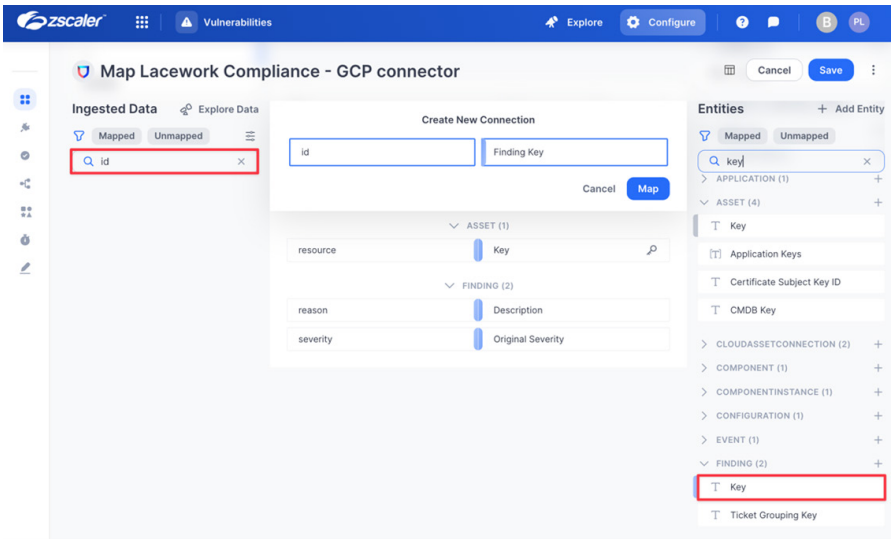

Figure 48. Id

   c. Click **Map**
6. Click **Save** then **Continue Anyway**.
7. On the **Sources** page, click **Process Now** > **Process Now under your Lacework Compliance—GCP Data Source**.
8. From the **Vulnerabilities** tab in the **Zscaler UVM** dashboard (Remediation Hub):
   a. In the left pane, select **Settings** > **Score**.
   b. Click **Add Factor** in the **Risk & Mitigating Factors** section.
9. In the **Add new factor** modal:
   a. **Factor Type**: Select **Risk Factors** (**Mitigating Factors** generally lower risk scoring, while **Risk Factors** generally increase risk scoring).
   b. **Factor Name**: Provide a name (e.g., `Finding Original Severity`).
   c. **Field**: Choose **Finding Original Severity**.
   d. **When Finding Original Severity Equals**: Enter **Critical** and enter a percentage by which the risk is increased. This example uses 10%.

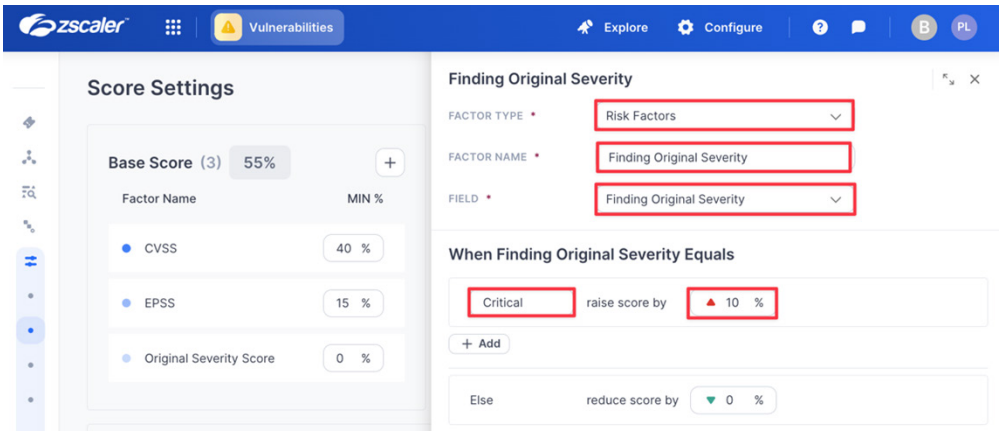

Figure 49. Add new factor

10. Click **Apply**, then **Save & Run**.
11. In the left-side pane, select the **Findings** dashboard. From the **Findings** dashboard:
    a. Set a **Severity = Critical** filter by clicking **Severity** and clicking **Critical**.
    b. Click one of your **Lacework Compliance—GCP Findings** in the filtered list.
    c. In the **Finding** modal that appears, click the **Details** tab.
    d. Click the **Finding**.
    e. Review the output (notice the **Score Adjustment** section and how **Finding Original Severity** has modified the risk scoring).

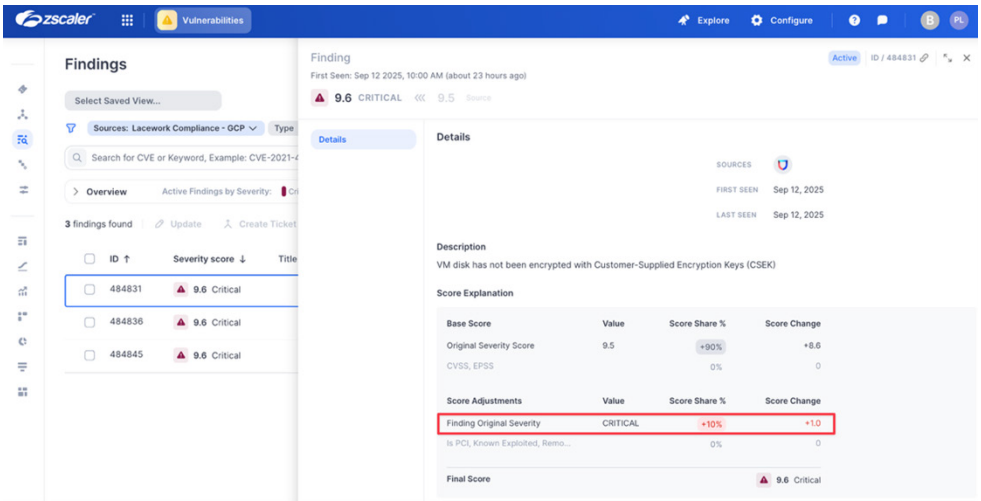

Figure 50. Finding Original Severity

Appendix A: Requesting Zscaler Support

If you need Zscaler Support to provision certain services or to help troubleshoot configuration and service issues, it is available 24/7/365.

Support via ZIA

To contact Zscaler Support:

1. Go to **Administration** > **Settings** > **Company Profile**.

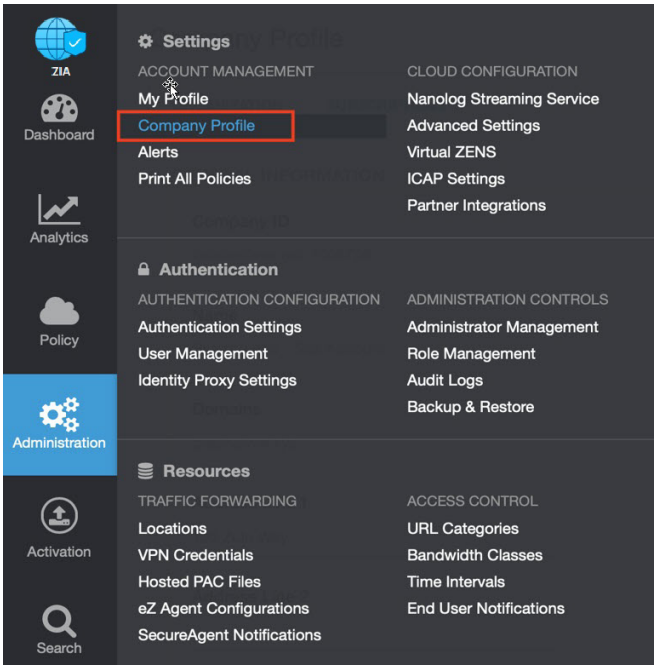

Figure 51. Collecting details to open support case with Zscaler TAC

2. Copy your **Company ID**.

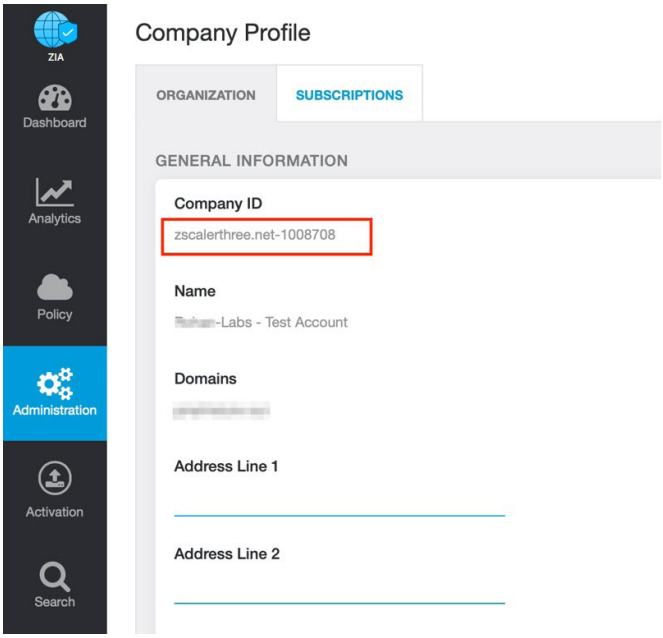

Figure 52. Company ID

3. With your company ID information, you can open a support ticket. Go to **Dashboard** > **Support** > **Submit a Ticket**.

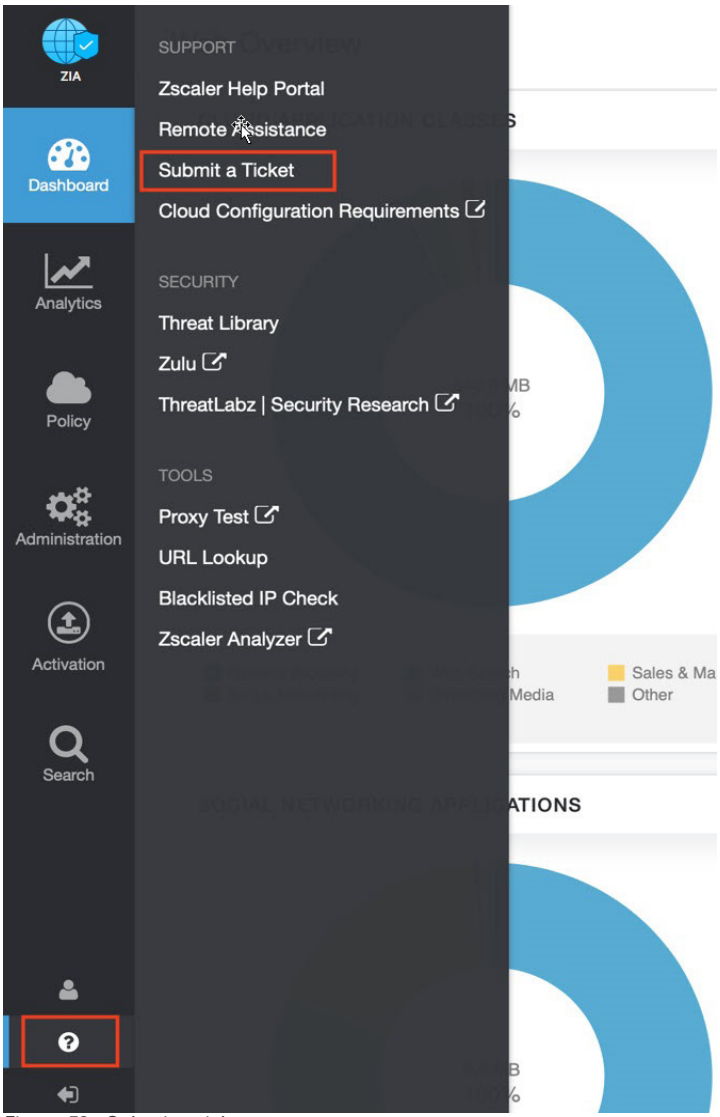

Figure 53. Submit a ticket

Support via Zscaler UVM

To contact Zscaler UVM Support:

1. Log in to the Zscaler UVM Platform.

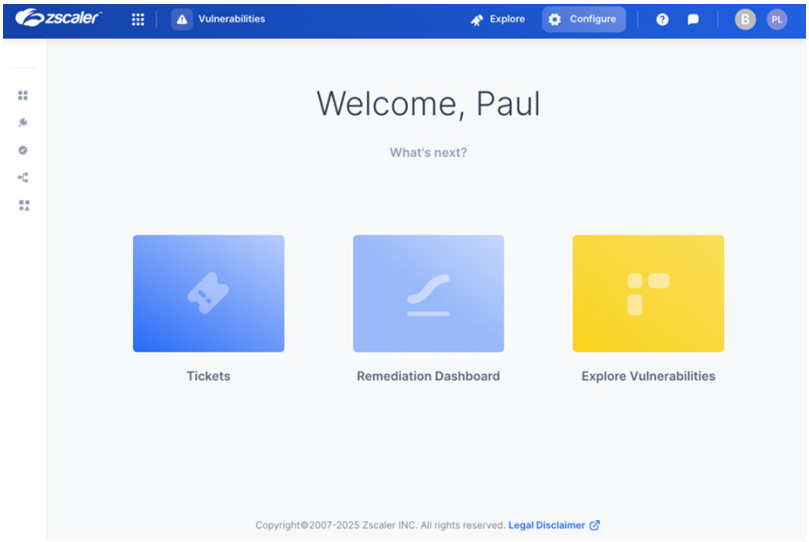

Figure 54. Zscaler UVM Admin Portal

2. Click **Contact Support**.

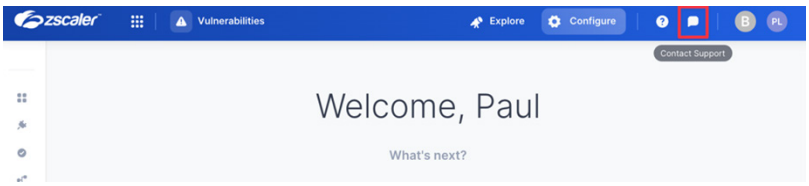

Figure 55. Contact Support

3. Complete the details in the **Contact us** form and click **Send**.

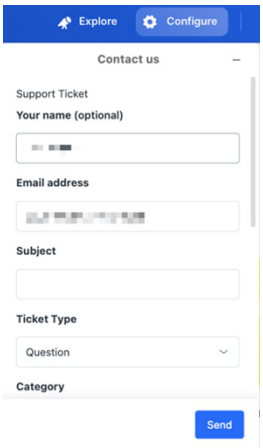

Figure 56. Contact us