## Contents

### Terms and Acronyms 3

### About This Document 4

- **Zscaler Overview** 4
  - Zscaler Internet Access (ZIA) Overview 4
  - Zscaler Private Access (ZPA) Overview 4
  - Zscaler Resources 4

- **Elastic Overview** 5
  - Arctic Wolf Platform Overview 5
  - Arctic Wolf Resources 5

- **Audience** 5

- **Software Versions** 5

- **Request for Comments** 5

### Syslog Configuration for Zscaler 6

- **Configure Zscaler Nanolog Streaming Service** 6

### Appendix A: Requesting Zscaler Support 8

- **Gather Support Information** 8
  - Save Company ID 8
  - Enter Support Section 9
**Terms and Acronyms**

The following table lists the terms and acronyms referenced in this guide.

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>CA</td>
<td>Central Authority (Zscaler)</td>
</tr>
<tr>
<td>CSV</td>
<td>Comma-Separated Values</td>
</tr>
<tr>
<td>DPD</td>
<td>Dead Peer Detection (RFC 3706)</td>
</tr>
<tr>
<td>GRE</td>
<td>Generic Routing Encapsulation (RFC2890)</td>
</tr>
<tr>
<td>IKE</td>
<td>Internet Key Exchange (RFC2409)</td>
</tr>
<tr>
<td>IPSec</td>
<td>Internet Protocol Security (RFC2411)</td>
</tr>
<tr>
<td>PFS</td>
<td>Perfect Forward Secrecy</td>
</tr>
<tr>
<td>PSK</td>
<td>Pre-Shared Key</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Socket Layer (RFC6101)</td>
</tr>
<tr>
<td>XFF</td>
<td>X-Forwarded-For (RFC7239)</td>
</tr>
<tr>
<td>ZIA</td>
<td>Zscaler Internet Access (Zscaler)</td>
</tr>
<tr>
<td>ZEN</td>
<td>Zscaler Enforcement Node (Zscaler)</td>
</tr>
<tr>
<td>ZPA</td>
<td>Zscaler Private Access (Zscaler)</td>
</tr>
</tbody>
</table>
About This Document

This section describes the companies, products, and requirements for the integration referenced in this 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. For more information on Zscaler, visit Zscaler’s webpage or follow Zscaler on Twitter @zscaler.

Zscaler Internet Access (ZIA) Overview

Zscaler Internet Access (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, CASB, and Browser Isolation, allowing you to start with the services you need now and activate others as your needs grow.

Zscaler Private Access (ZPA) Overview

Zscaler Private Access (ZPA) is a cloud service that provides secure remote access to internal applications running on 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, a piece of software called Zscaler Client Connector is installed. Zscaler Client Connector ensures the user’s device posture and extends a secure micro-tunnel out to the Zscaler cloud when a user attempts to access an internal application.

Zscaler Resources

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ZIA Help Portal</td>
<td>Help articles for ZIA.</td>
</tr>
<tr>
<td>ZPA Help Portal</td>
<td>Help articles for ZPA.</td>
</tr>
<tr>
<td>Zscaler Tools</td>
<td>Troubleshooting, security and analytics, and browser extensions that help Zscaler determine your security needs.</td>
</tr>
<tr>
<td>Zscaler Training and Certification</td>
<td>Training designed to help you maximize Zscaler products.</td>
</tr>
<tr>
<td>Submit a Zscaler Support Ticket</td>
<td>Zscaler support portal for submitting requests and issues.</td>
</tr>
</tbody>
</table>
Elastic Overview

Arctic Wolf uses its the cloud-native Arctic Wolf® Platform to help organizations end cyber risk by providing security operations as a concierge service. Arctic Wolf solutions include Arctic Wolf® Managed Detection and Response (MDR), Managed Risk, Managed Cloud Monitoring, and Managed Security Awareness; each delivered by the industry’s original Concierge Security® Team. Highly-trained Concierge Security experts work as an extension of internal teams to provide 24×7 monitoring, detection, and response, as well as ongoing risk management to proactively protect organizations while continually strengthening their security posture. Visit Arctic Wolf’s website for more information.

Arctic Wolf Platform Overview

Built on an open XDR architecture, The Arctic Wolf Platform combines with our Concierge Security Model to work as an extension of your team. We provide 24×7 monitoring, detection, and response, ongoing risk management, as well as security awareness training to proactively protect your environment while continually strengthening your security posture.

Arctic Wolf Resources

The following table contains links to Arctic Wolf support resources.

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Arctic Wolf support portal</td>
<td>Arctic Wolf support portal for submitting requests and issues.</td>
</tr>
</tbody>
</table>

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, please refer to:

- Appendix A: Requesting Zscaler Support
- Zscaler Resources
- Arctic Wolf Resources

Software Versions

This document was authored using the latest version of ZIA and the Arctic Wolf Platform.

Request for Comments

- For prospects and customers: we value reader opinions and experiences. Contact us at 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.
Syslog Configuration for Zscaler

This document describes how to configure the Nanolog Streaming Service (NSS) to send syslog-formatted messages from Zscaler device(s) to your Arctic Wolf® sensor. Arctic Wolf supports the QRadar LEEF feed output type.

Before you begin, you need to have the Nanolog Streaming Service virtual appliance installed and configured to stream web logs from your Zscaler device(s). For more information, see About Nanolog Streaming Service (NSS) and Configuring Advanced NSS Settings on the Zscaler Help Portal.

Configure Zscaler Nanolog Streaming Service

To configure your Zscaler NSS:

1. Access your Zscaler NSS web administration interface and log in with appropriate credentials.
2. Select Administration > Settings > Nanolog Streaming Service to access the Nanolog Streaming Service page.
3. Select the NSSFeeds tab and then click Add.
4. Complete the following steps to create a new NSS feed:
   a. In the Feed Name text box, enter a descriptive title for the feed (for example, AWN Syslog).
   b. Select the appropriate server from the NSS Server box.
   c. Under Status, select Enabled.
   d. Set the SIEM IP Address to the management IP address of the Arctic Wolf sensor.
   e. Set the SIEM TCP Port to 514.
   f. Verify that the Log Type is set to Web Log.
   g. Set the Feed Output Type to QRadar LEEF. The Feed Output Format box is populated with the appropriate string.

Figure 1. Add NSS Feed window
5. Leave the remaining fields in this dialog box at their default values. We suggest leaving User Obfuscation set to Disabled to allow your Concierge Security® Team (CST) to correlate these events with additional user actions in your environment. Additionally, leave the Timezone at its default of GMT, and confirm that the Duplicate Logs setting is set to Disabled.

6. Click Save. You have successfully configured your Zscaler Nanolog Streaming Service to send syslog-formatted messages to your Arctic Wolf sensor.

7. Create a ticket for your CST advising that you have completed this configuration, as well as the IP address assigned to the NSS virtual machine. Your CST will confirm when Arctic Wolf is successfully processing logs from the Zscaler device(s).
Appendix A: Requesting Zscaler Support

Gather Support Information

You might need Zscaler support for provisioning certain services, or to help troubleshoot configuration and service issues. Zscaler support is available 24/7 hours a day, year-round. To contact Zscaler support, select Administration > Settings > Company profile.

Save Company ID

Copy your Company ID.
Enter Support Section

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

![Submit a ticket](Figure 4. Submit a ticket)