Zero Trust Branch Connectivity with Zscaler Branch Connector

Reference Architecture

Contents

About Zscaler Reference Architectures Guides 3
- Who Is This Guide For? 3
- A Note for Federal Cloud Customers 3
- Conventions Used in This Guide 3
- Finding Out More 3
- Terms and Acronyms Used in This Guide 4
- Icons Used in This Guide 5

Introduction 6
- Key Features and Benefits 8
- New to Zscaler Branch Connector? 8

Understanding Zscaler Branch Connector Operation 9
- Non-Gateway/One-Arm Mode vs. Gateway Mode 10
- High Availability with Gateway Mode 12
- DNS Request Handling 13
- Branch Connector Sizing 14

Deploying and Operating Branch Connector 16
- API Key Management 16
- Predefined Forwarding Rules 16
- Location Templates 16
- Branch Configuration Templates 17
- Zero Touch Provisioning for Hardware-Based Branch Connectors 17
- VM Installation Steps 18
- Maintenance and Upgrades 18

Summary 19

About Zscaler 21

About Zscaler Reference Architectures Guides

The Zscaler™ Reference Architecture series delivers best practices based on real-world deployments. The recommendations in this series were developed by Zscaler's transformation experts from across the company.

Each guide steers you through the architecture process and provides technical deep dives into specific platform functionality and integrations.

The Zscaler Reference Architecture series is designed to be modular. Each guide shows you how to configure a different aspect of the platform. You can use only the guides that you need to meet your specific policy goals.

Who Is This Guide For?

The Overview portion of this guide is suitable for all audiences. It provides a brief refresher on the platform features and integrations being covered. A summary of the design follows, along with a consolidated summary of recommendations.

The rest of the document is written with a technical reader in mind, covering detailed information on the recommendations and the architecture process. For configuration steps, we provide links to the appropriate Zscaler Help site articles or configuration steps on integration partner sites.

A Note for Federal Cloud Customers

This series assumes you are a Zscaler public cloud customer. If you are a Federal Cloud user, please check with your Zscaler Account team on feature availability and configuration requirements.

Conventions Used in This Guide

The product name ZIA Service Edge is used as a reference to the following Zscaler products: ZIA Public Service Edge, ZIA Private Service Edge, and ZIA Virtual Service Edge. Any reference to ZIA Service Edge means that the features and functions being discussed are applicable to all three products. Similarly, ZPA Service Edge is used to represent ZPA Public Service Edge and ZPA Private Service Edge where the discussion applies to both products.

Notes call out important information that you need to complete your design and implementation.

Warnings indicate that a configuration could be risky. Read the warnings carefully and exercise caution before making your configuration changes.

Finding Out More

You can find our guides on the Zscaler website at Reference Architectures (https://www.zscaler.com/resources/reference-architectures).

You can join our user and partner community and get answers to your questions in the Zenith Community (https://community.zscaler.com/).

Terms and Acronyms Used in This Guide

Acronym	Definition
AUP	Acceptable Use Policy
CARP	Common Address Redundancy Protocol
DTLS	Datagram Transport Layer Security
FQDN	Fully Qualified Domain Name
HA	high availability
IoT	Internet of Things
OT	operational technology
SASE	Secure Access Service Edge
SD-WAN	Software-Defined Wide Area Network
TLS	Transport Layer Security
VM	virtual machine
XFF	X-Forwarded-For
ZIA	Zscaler Internet Access™
ZPA	Zscaler Private Access™
ZTE	Zero Trust Exchange™
ZTP	Zero Touch Provisioning

Icons Used in This Guide

The following icons are used in the diagrams contained in this guide.


Headquarters


Branch Office


Firewall

Virtual Private Network


Cloud


Router


Client


Application


Branch Connector

Zscaler Zero Trust Exchange

Introduction

For more than a decade, Software-Defined Wide Area Network (SD-WAN) has become the preferred model for branch connectivity. While the deployment models and traffic flows differ by vendor, all involve leveraging low-cost consumer internet paired with more expensive site-to-site VPN links to centralized applications and security appliances.

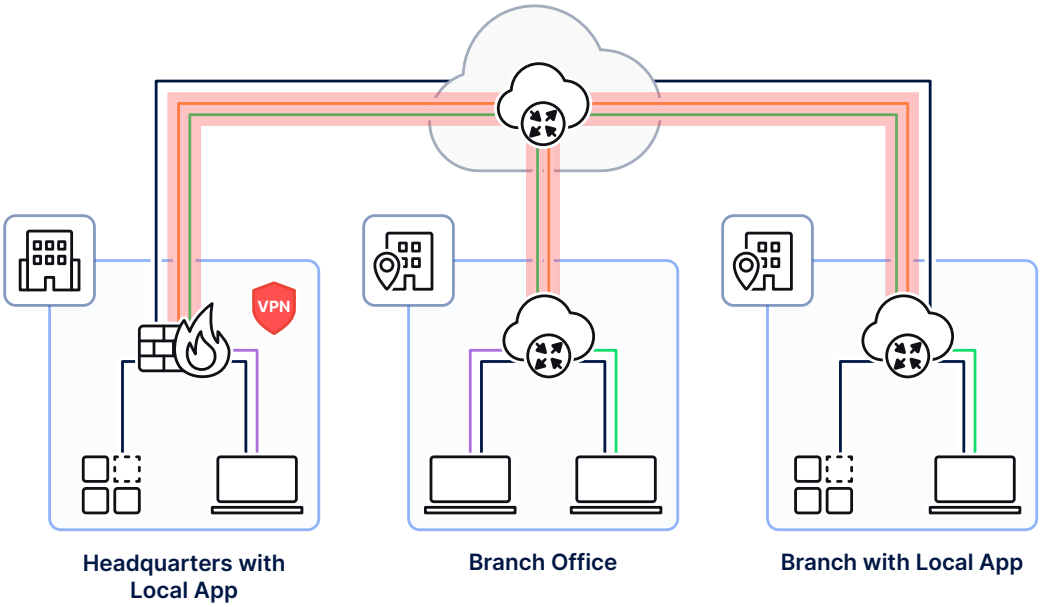

Figure 1: SD-WAN extends your network to your branch locations while also leveraging consumer-grade internet access

At the branch level, SD-WAN is an extension of the organization's network. From the user perspective, there is little difference between being at a branch location versus the headquarters location. For IT staff, this means configuring firewalls and route tables across the organization. Users at the branch location are on a local network, usually with the ability to move horizontally. The shift to the cloud and Zero Trust security is affecting these SD-WAN models.

With most of your applications and data stored outside of your organization, it makes more sense for users to go to the geographically closest instance of that resource. Going directly to the internet instead of backhauling data for security inspections has its own costs. You need to increase the level of inspection at the branch location, which means more boxes, maintenance contracts, and configuration overhead.

Organizations also want to reduce their attack surface and restrict access to information. Zero Trust security offers a more managed branch location and devices, with more security checks on user and application access. With a highly mobile and remote user base, the complexity of network access and security often conflict.

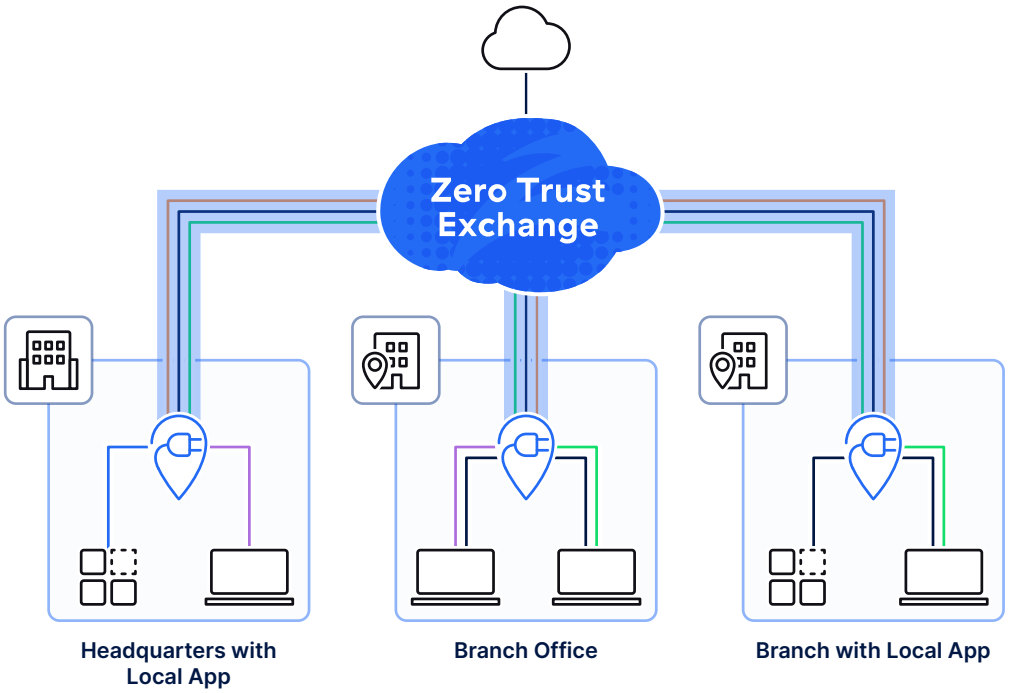

Figure 2: Zscaler Branch Connector provides plug-and-play access to the Zero Trust Exchange

Zscaler Branch Connector takes a different approach to the SD-WAN model. It starts with a Zero Trust approach to the branch office, using the Secure Access Service Edge (SASE) model. Leveraging both Zscaler Internet Access (ZIA) and Zscaler Private Access (ZPA), users gain access to applications, not networks. Designed to be deployed anywhere, from small branches to large campuses and data centers, Zscaler Branch Connector simplifies connecting your devices with the Zscaler cloud, the Zero Trust Exchange (ZTE).

Deployment occurs in either a hardware appliance at branch locations, or as a virtual machine (VM) in your data centers. Physical installation of the hardware is plug and play, with standard gigabit Ethernet ports and an AC power supply. When deployed, your traffic is tunneled to the Zscaler cloud using Datagram Transport Layer Security (DTLS) for ZIA Transport Layer Security (TLS) for ZPA.

When deploying Branch Connector as a hardware platform, security of the physical device is very important. Zscaler leverages a TPM 2.0 chip for secure authentication of the device. The TPM chip is also leveraged to provide the Zero Touch Provisioning (ZTP) agent authentication credentials to the Zscaler cloud, and then to download the provisioning template.

Deploying Branch Connector helps to simplify your network and ensure all of the devices in your branch location can access the Zscaler platform. This includes Internet of Things (IoT) and operational technology (OT) tools that can be connected without the need to install an agent.

Similarly, deploying Branch Connector during M&A activities allows you to provide access to your internal applications with the merged or acquired company within hours, instead of days, weeks, or months later.

Zscaler Branch Connector also enables you to replace your legacy site-to-site VPN deployments. Your applications are available via ZPA to all of your authorized users. You can also eliminate VPN and jump-host access to your OT systems with ZPA. Additionally, your Branch Connector instance can act as an App Connector for local systems and applications, providing secure remote access.

Key Features and Benefits

- Enables Zero Trust everywhere for all users, devices, servers, and IoT/OT, regardless of location or cloud.
- Improves application performance and increases productivity by replacing complex site-to-site VPNs with a simple direct-to-cloud architecture.
- Minimizes the internet attack surface by placing private applications behind the ZTE, where they cannot be discovered or attacked from the internet.
- Prevents lateral threat movement by connecting directly to applications, not the network.
- Enables organizations to discover and classify IoT devices with automatic device classification based on traffic profiles.
- Simplifies secure access to OT resources with clientless browser-based access to SSH/RDP/VNC ports on OT assets.
- Enforces finely grained forwarding policies for internet and non-internet traffic using ZIA or ZPA.
- Introduces plug-and-play deployment with ZTP, which simplifies deployment and reduces time to integration.

New to Zscaler Branch Connector?

- To learn more about Zscaler's approach to the Zero Trust branch, see Why Settle for Traditional SD-WAN? (https://www.zscaler.com/products-and-solutions/zero-trust-sd-wan).
- Read our blog Introducing Zero Trust SASE (https://www.zscaler.com/blogs/product-insights/introducing-zero-trust-sase).
- Read our online documentation at What Is Zscaler Branch Connector? (https://help.zscaler.com/cloud-branch-connector/what-zscaler-branch-connector).
- For additional forwarding methods, see Traffic Forwarding in Zscaler Internet Access (https://www.zscaler.com/resources/reference-architectures/traffic-forwarding-zia.pdf).

Understanding Zscaler Branch Connector Operation

Branch Connector is designed to simply move your traffic through the ZTE cloud for inspection and policy enforcement. When connected, Branch Connector establishes a connection to the ZTE cloud. Your users and devices then connect to the internet and your private applications by passing through the Branch Connector. The traffic is examined and, depending on destination and policy, forwarded to the appropriate Zscaler service, routed directly, or dropped.

Branch Connector can operate in one of two modes: forwarding of traffic using non-gateway mode (also called one-arm mode), and gateway mode. In non-gateway/one-arm mode, traffic is passed to Zscaler services as appropriate, but another router on your network is responsible for redirecting traffic to Branch Connector and terminating your ISP connections. In gateway mode, Branch Connector takes the place of the router, providing the following services:

- NAT services
- Edge and inter-VLAN firewall capabilities
- Multiple ISP termination
- Load balancing across multiple ISP links
- Monitoring link health

For Branch Connector to provide access to ZPA application segments to your non-user devices, it must see the DNS requests made by all your devices. This allows Branch Connector to forward the requests to ZTE or your local DNS server. Branch Connector can then provide resolution for your private applications that exist behind ZPA. This is especially important when Branch Connector is not your default gateway.

In gateway mode, Branch Connector can also act as your DNS gateway when there is no local DNS at the branch location. In this mode, the Branch Connector intercepts DNS requests from devices in the LAN. Branch Connector forwards DNS requests for ZPA application segments to the DNS gateway, and forwards DNS requests to other resolvers. The other resolvers used for forwarding can be either dynamically learned from WAN DHCP or defined as DNS gateway values.

Branch Connector can include the option to run an instance of App Connector within the Branch Connector platform. This enables you to provide access to local applications, tools, and devices such as OT platforms. The App Connector learns about local services behind the Branch Connector, and when they are discovered, you can then authorize users to connect to the local services.

When the Branch Connector boots, it authenticates itself using the ZTP service to the Zscaler cloud. It establishes a DTLS connection to ZIA and a TLS connection to ZPA. If the DTLS tunnel connection cannot be established, a TLS tunnel is formed to ZIA. The certificate embedded in the chip is mapped to the device's serial number during the manufacturing process. This ensures that your device connects to your tenant in the Zscaler cloud and downloads the correct configuration files.

When a user sends traffic destined for the internet or a private address, the Branch Connector forwards the traffic based on one of the four conditions you select in your Traffic Forwarding policy:

- **Forward to ZIA** – Pass internet-bound traffic to ZIA for inspection.
- **Forward to ZPA** – Pass traffic bound for internal applications to ZPA.
- **Direct** – Send the traffic directly; do not use Zscaler Services.
- **Drop** – The request is dropped.

Typically, you send most traffic through either ZIA or ZPA for inspection and processing. If you have managed devices running Zscaler Client Connector, you should bypass the DTLS tunnel on Branch Connector. Zscaler Client Connector builds its own tunnels to ZIA and ZPA for each device when not on one of your established networks. Having these client devices directly connect to the Zscaler cloud allows you to preserve user authentication and device posture. It saves Branch Connector tunnel bandwidth for those applications and devices that do not have Zscaler Client Connector installed.

Non-Gateway/One-Arm Mode vs. Gateway Mode

Deciding between non-gateway/one-arm mode and gateway mode depends on your local branch design. It also depends on which devices should provide various services to the location. For a small branch or retail location, gateway mode is likely the easiest to manage and deploy without onsite IT. In a large campus or data center, non-gateway/one-arm mode might be more appropriate, with other dedicated routers handling the traffic flows in and out of the organization.

Gateway mode is often the correct choice, making the Branch Connector the layer 3 gateway for the local network. But in some cases, such as M&A access or IoT/OT visibility and control, the non-gateway/one-arm mode might be sufficient to route those devices across to the Zscaler cloud.

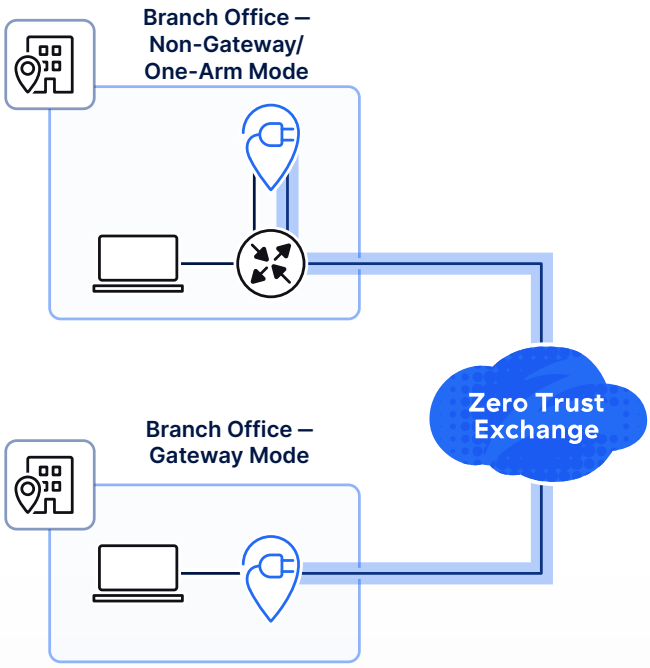

Figure 3: Branch Connector can be deployed as a forwarder or as your local network gateway

Non-Gateway/One-Arm Mode

In forwarding mode, you must make a design choice about what specific traffic will be forwarded to the Branch Connector. To redirect this traffic to Branch Connector, you can employ techniques such as Policy-Based Routing or Conditional DNS Forwarding. Other traffic that is not specific should be routed normally in your network. In this model, traffic is forwarded to the Branch Connector, encapsulated in the tunnel, and then sent on to the ZTE. Routing and networking are handled by existing equipment in your network without modification.

In non-gateway/one-arm mode, your network must have an external router on the network that can handle connections to your ISP.

Gateway Mode

In gateway mode, the Branch Connector hardware device becomes the default gateway for the local network. In this mode, Branch Connector supports dual ISP connectivity and high availability (HA) deployments. The Branch Connector can act as your DHCP server and support 802.1Q VLAN tagging of traffic. All user traffic passes through the Branch Connector, providing secure access for all devices and users.

In gateway mode, the following additional features are available:

LAN

- Connect to multiple L3 LAN networks and act as the default gateway for those networks.
- Provide a DHCP server for the local LAN segments. The DHCP server allows you to configure the following:
  - Address range
  - Default lease time
  - Maximum lease time
  - DHCP options, including default gateway, domain suffix, and DNS servers
  - Static lease addresses
- Static routing, with up to 32 static routes on the LAN side.
- Support for up to 20 VLANS (ZT-400) or 40 VLANs (ZT-600 and ZT-800) with 802.1Q VLAN tagging.
- Default inter-VLAN stateful traffic filtering rule that is dynamically created. This policy is disabled by default.
- Determine default gateway for ZIA independently for each WAN interface.

WAN

- Support for dual WAN uplinks, including multiple ISP support.
- ISP WAN uplink path monitoring.
- DHCP client support for dynamic ISP IP addressing.

High Availability

- WAN link redundancy with failover triggered by ISP WAN monitoring. WAN links can be set to active/active or active/standby.
- Hardware redundancy enabled via the Common Address Redundancy Protocol (CARP) shared between devices.
- DHCP server redundancy via a single pool of servers shared across a high availability pair of branch controller devices.

Traffic Forwarding

- ZIA
- ZPA
- Direct
- Drop
- Application-aware path selection

Gateway mode is only supported on hardware-based Zero Trust appliances.

High Availability with Gateway Mode

Branch Connector high availability (HA) comes in two forms: redundancy at the hardware device level, and redundancy at the WAN link level.

Branch Connector Hardware Redundancy

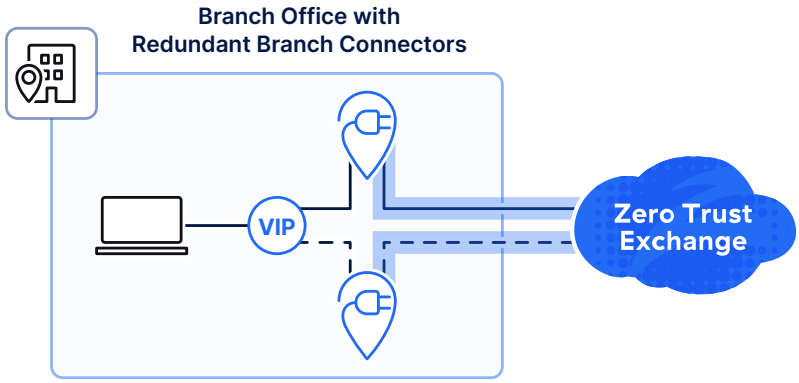

Figure 4: Zscaler Branch Connector hardware can operate in an active/standby redundancy model

When operating Branch Connector in a hardware deployment, you can run two physical instances of the hardware sharing a CARP VIP address on a per LAN subnet basis. The two Branch Connectors operate in an active/standby mode with no state sync between them. When the primary Branch Connector becomes unresponsive, the CARP address shifts to the backup Branch Connector.

For more information on configuring CARP and redundancy, see Branch Connector Deployment Management (https://help.zscaler.com/cloud-branch-connector/deployment-management/branch-connector-deployment-management).

WAN Link High Availability

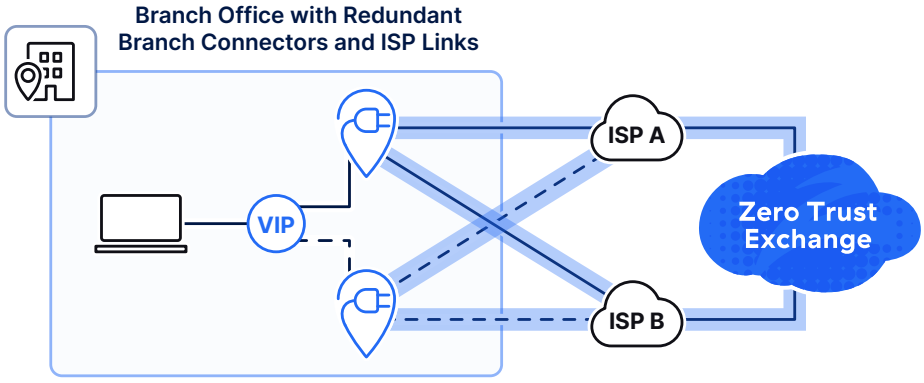

Figure 5: Redundant WAN links and link health monitoring provide automatic failover

WAN link level and redundancy involves the ISP links, with each Branch Connector in gateway mode able to monitor and use two WAN links. These can be configured in either active/active or active/standby modes. When configuring your traffic forwarding profile, you select between Balanced or Best Link if there are two ISP links available.

The Branch Connector uses link monitoring to determine the best link and ensure that there is an active path on each ISP link. Link monitoring works by sending a TCP probe to the nearest ZIA proxy VIP address on port 443. The Branch Connector, in turn, uses the response to calculate a link health score based on packet loss, latency, and jitter.

For more information on configuring WAN link redundancy, see Configuring a Branch Configuration Template (https://help.zscaler.com/cloud-branch-connector/configuring-branch-configuration-template#GatewayWAN).

Branch Connector VMware Redundancy

Running Branch Connector VMs in a redundant model operates similarly to their hardware counterparts. The main difference is with VMware, which requires additional configuration of the hypervisor. These settings allow the shared IP address and failover to function. To view the most current recommendations, see Deploying Branch Connector & App Connector on VMware Platforms (https://help.zscaler.com/cloud-branch-connector/deploying-branch-connector-app-connector-vmware-platforms#Prereqs).

DNS Request Handling

When processing a DNS request, the Branch Connector forwards the request based on your DNS policy. The policy is evaluated in a top-down, first-match manner. The following list outlines the response based on the forwarding action that is matched in your policy:

- **Resolved by ZPA** – The DNS request arrives at the Branch Connector on any destination IP address, for a fully qualified domain name (FQDN) or wildcard domain name, and the request matches a ZPA application. Branch Connector intercepts requests and responds with a customer-defined synthetic IP address from the customer-defined IP pool.
- **Allow** – The DNS request arrives at the Branch Connector from a device configured with a custom DNS server destination IP address (e.g., 8.8.8.8). Branch Connector encapsulates the request with a client

source IP address and destination DNS IP address (e.g., 8.8.8.8) and forwards the request based on the configured Traffic Forwarding policy. If the Branch Connector receives a DNS request destined to 8.8.8.8, the DNS policy action is set to "Allow" and the Traffic Forwarding policy that matches this flow is set to "Forward to ZIA", then the DNS transaction is sent to ZIA.

- **Block** – DNS requests that match the rule are silently dropped.
- **Redirection Request** – DNS requests matching the policy are redirected to the specified DNS Gateway. You can configure up to two DNS server IP addresses.

For more information, see Configuring a DNS Filtering Rule (https://help.zscaler.com/cloud-branch-connector/configuring-dns-filtering-rule).

Branch Connector Sizing

Branch Connector is available in both hardware and VM versions. Selecting the right version of Branch Connector hardware is based on the available tunnel throughput of each model. This tunnel contains all the traffic sent between your branch site and the Zscaler data center where the tunnels from the Branch Connector are terminated.

For VM deployments, speed is primarily determined by the host and the deployed VM size. Branch Connector supports both VMware and Linux KVM platforms. The software is dependent on the size of the VM deployed.

Determining Location Bandwidth

When deploying Branch Connector, you must determine how much bandwidth each of your locations sends through Zscaler services. This first step in selecting the appropriate device is to measure the overall bandwidth you will send and receive from Zscaler. When calculating the throughput requirements, you must include:

- Your regular user traffic that is destined for ZIA inspection, unless that data will be carried directly via Zscaler Client Connector tunnels.
- Any inbound ZPA traffic to an App Connector running on the Branch Connector.
- Any guest user traffic that might be sent for inspection.
- Any IoT/OT traffic that is sent through Zscaler.

Selecting the Appropriate Branch Connector Hardware or Virtual Machine

Using the total bandwidth for the location, you can select the required model using the Tunnel Throughput column in the following table. You should also consider the connection speed to the branch and any expected growth in devices or services that might impact your calculations.

Model	HW / SW	Tunnel Throughput	Number of GE Ports	Use Case
ZT-400	Hardware	200 Mbps	4	Small branches
ZT-600	Hardware	500 Mbps	6	Small to medium branches
ZT-800	Hardware	1 Gbps	8	Medium to large branches
VM	Software	Multi-Gig	N/A	Large campus and data center

Table 1: Zscaler Branch Connector hardware and software sizing, note one interface is reserved for management

Branch Connector VM requirements are the same across VMware and Linux KVM deployments. The requirements increase if an instance of App Connector is also running inside of the Branch Connector. The following table summarizes the requirements for small- and medium-sized deployments.

Deployment Model	Size	Memory	CPU Cores	Data Disk	NICs
Branch Connector	Small	4 GB	2	128 GB	2
	Medium	8 GB	4	128 GB	4
Branch Connector and App Connector	Small	16 GB	4	128 GB	3
	Medium	32 GB	6	128 GB	5

Table 2: Branch Connector VM sizing guidelines

Deploying and Operating Branch Connector

Branch Connector devices leverage a series of configuration templates to deploy and manage both hardware and VMs. Each device relies on a series of templates that outlines its operation. This is also leveraged by a zero-touch provisioning process that allows the Zero Trust appliance to boot and operate.

API Key Management

Your Zscaler services leverage an API key to allow devices to connect to your Zscaler tenant. This API key is initially generated by Zscaler, but you can regenerate it with a random string or enter a string of your own. There is only one API key per tenant at any one time.

To learn more about API key management, see Managing Organization API Keys (https://help.zscaler.com/cloud-branch-connector/managing-organization-api-keys).

Predefined Forwarding Rules

To speed up your deployments, Zscaler has built a set of traffic forwarding rules. These rules cover traffic forwarding for LAN traffic, WAN traffic, and traffic destined for Zscaler domains. Each of these rules has an associated dynamic IP group. These groups are populated by the ZIA Public Service Edge devices as they receive traffic.

These rules use dynamic destination groups and are populated by the Branch Controller:

- **LAN Destination Group** – LAN-connected and static routes
- **WAN Destination Group** – WAN-connected routes
- **Zscaler Cloud Endpoints** – Zscaler domains, IP addresses, Virtual IP addresses, and FQDNs

By default, these rules are disabled. You can enable them to allow traffic to go direct when it matches criteria. Using the Zscaler cloud endpoints, any traffic from a device with Zscaler Client Connector is routed directly to Zscaler. This saves your Branch Controller tunnel bandwidth for those stations that cannot run Zscaler Client Connector.

Learn more at About Traffic Forwarding (https://help.zscaler.com/cloud-branch-connector/about-traffic-forwarding)

Location Templates

When you deploy a Branch Connector, a new location is created that leverages location templates. The location template contains choices that you make about your network operations. These preferred default settings are:

- **Enable XFF Forwarding** – Enable if you want the Zscaler service to use the X-Forwarded-For (XFF) headers that your on-premises proxy server inserts in outbound HTTP requests.
- **Enforce Authentication** – Enable to require users from this location to authenticate to the service.
- **Enable Caution** – Enable to display an end user notification for unauthenticated traffic. If disabled, the action is treated as an allow policy.

- **Enable AUP** – Enable to display an Acceptable Use Policy (AUP) for unauthenticated traffic and require users to accept it. If you enable this setting, the Custom AUP Frequency (Days) field appears. Specify in days how frequently the AUP is displayed to users.
- **Enforce Firewall Control** – Select to enable the service's firewall controls. If you enable this setting, the Enable IPS Control setting appears. Select this setting to enable IPS controls for the location template. To enable IPS control, you must subscribe to the advanced firewall SKU.
- **Enforce Bandwidth Control** – Enable to specify the maximum bandwidth limits for Download (Mbps) and Upload (Mbps).

To learn more about using location templates, see About Location Templates (https://help.zscaler.com/cloud-branch-connector/about-location-templates).

Branch Configuration Templates

Branch Connector devices use branch configuration templates to understand their location, Branch Connector groups, and network configurations. For VM instances, only non-gateway/one-arm mode deployments are supported. For Zscaler hardware-based Branch Connector devices, deployment can occur in either non-gateway/one-arm mode or gateway mode.

Common to both modes are basic information such as the template name, location, location templates, Branch Connector groups, management interface details, and App Connector functionality. If you follow the recommended best practices and deploy in an HA configuration, you must also manually set up the management and forwarding interfaces.

If you select gateway mode on a hardware Branch Connector, you must configure additional WAN and LAN settings. For local networking settings, you must configure items including the local DHCP pools for LAN devices, VLANs and associated sub-interfaces, and DNS server settings. Routing is also available on the LAN side, supporting 32 static routes. The WAN side requires that you configure the interfaces for up to two ISP connections.

For more information on branch configuration templates, see Configuring a Branch Configuration Template (https://help.zscaler.com/cloud-branch-connector/configuring-branch-configuration-template).

Zero Touch Provisioning for Hardware–Based Branch Connectors

Zscaler's hardware-based Branch Connector devices leverage a TPM chip with built-in certificates to authenticate the hardware device. This is leveraged when setting up new Branch Connector devices that are shipped directly to their end location to be installed and configured automatically.

In this mode, the Branch Connector reaches out to the Zscaler Zero Touch Provisioning (ZTP) site for configuration updates. The ZTP site challenges the Branch Connector by using certificates to authenticate the device. The certificates are mapped to the device's serial number, which is associated with your Zscaler tenant.

ZTP is only available for hardware-based Branch Connector models. For VM devices, you manually input the device URL when provisioning the VM.

You can learn more about manual hardware installation at Installing Zero Trust Branch Devices (https://help.zscaler.com/cloud-branch-connector/installing-zero-trust-branch-devices).

VM Installation Steps

Zscaler provides detailed configuration steps for each supported platform on the Zscaler Help site:

- Deploying Branch Connector on VMware Platforms (https://help.zscaler.com/cloud-branch-connector/deploying-branch-connector-vmware-platforms)
- Deploying Branch Connector with Linux KVM (https://help.zscaler.com/cloud-branch-connector/deploying-branch-connector-linux-kvm)

Maintenance and Upgrades

For redundancy during upgrades, Branch Connector is installed in pairs at each location.

Branch Connector runs the Zscaler OS in the VM. Software updates and OS updates are provided by Zscaler via automatic upgrades. When a Branch Connector is deployed, you select the date and time the upgrade will occur on a weekly basis. The default is Sunday at midnight local time.

This automatic check and update means it is critical that your Branch Connector locations are accurate. An inaccurate location can lead to upgrades occurring in the middle of the day. Always specify exactly where the Branch Connector is located when deploying the VM.

You can configure this upgrade window from the Branch Connector Portal. Zscaler recommends that Branch Connector appliances be deployed as redundant HA instances. The Zscaler software upgrade process upgrades one instance of a pair at a time, providing availability for the location with the remaining Branch Connector.

VMs and the Shared Responsibility Model

Zscaler handles updating the operating systems of hardware Branch Connectors and VM software for images. However, you are responsible for maintaining the VM hosting environment with software updates and patches as appropriate for your platform.

Summary

Zscaler Branch Connector simplifies the connection back to the Zscaler cloud. Branch Connector provides Zero Trust access to applications following the SASE model. You can eliminate traditional SD-WAN offerings that provide network access, and instead move to an application access model. Branch Connector centralizes management and logging in a single platform.

This simplified access also reduces your network overhead, freeing you from managing routers and GRE connections. Instead, Zscaler's plug-and-play hardware devices accelerate onboarding of your branch offices and devices. For larger campuses and data centers, Zscaler offers VM-based Branch Connector software images for both VMware and Linux KVM platforms.

By extending Zscaler's Zero Trust security services to the network edge, you can eliminate costly and complex site-to-site VPN connections. If your branches have services that others need to access, you can leverage a built-in App Connector on the Branch Connector with ZPA to provide access. Branch Connector sits between your devices and apps, identifying IoT devices that you might not have known about.

M&A activities can provide value with immediate access to applications without touching any devices. By plugging in a Branch Connector at your organization's sites, all authorized users have access to your internal applications. This enables you to rapidly combine teams, while IT focuses on combining the network technology for optimum performance.

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange™ protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SASE-based Zero Trust Exchange is the world's largest inline cloud security platform.