Getting Started

This chapter provides you with a brief overview of the Cisco Secure Firewall features and the supported SD-WAN capabilities.

About This Publication

This guide details the primary use cases that uses the SD-WAN capabilities supported on Cisco Secure Firewall.

The approaches do not address all of the possible network needs; instead, they provide models on which you can pattern your network. You can choose not to use features presented in the examples, or you can add or substitute features that better suit your needs.

This guide assumes you are familiar with Cisco Secure Firewall. For more information on configurations, see Cisco Secure Firewall Management Center Administration Guide, 7.3 and Cisco Secure Firewall Management Center Device Configuration Guide, 7.3.

Cisco Secure Firewall

Cisco Secure Firewall is an exceptionally robust firewall solution with cutting-edge features such as Snort IPS, URL filtering, and malware defense.

This comprehensive offering greatly simplifies threat protection by enforcing consistent security policies across physical, private, and public cloud environments.

Furthermore, it grants extensive visibility into your network infrastructure, swiftly identifying the origin and activity of potential threats. Armed with this knowledge, you can promptly take action to stop attacks before they have a chance to disrupt your operations.

In addition to traditional firewall capabilities, it provides features as:

1. Application visibility and control
2. User identity awareness and control
3. Intrusion prevention and intrusion detection

4. SSL/TLS decryption
5. Reputation based blocking
6. File and malware protection
7. Virtual Private Network (VPN)

To further secure network deployments, Cisco Secure Firewall provides additional security capabilities in its later releases such as:

- Encrypted Visibility Engine (EVE) that enhance encrypted traffic inspection without the need to implement full main-in-the-middle (MITM) decryption.
- Elephant Flow Detection to detect and remediate elephant flows (flows that are typically larger than 1 GB/10 seconds) and avoid high CPU utilization and packet drops.
- Cisco Secure Dynamic Attribute Connector (CSDAC) that brings agility and intelligence into your security policy management by leveraging tags and labels for policy configuration rather than traditional IP/network-based policy configuration.

Overview of SD-WAN Capabilities

Software-Defined WAN (SD-WAN) solutions replace traditional WAN routers and are agnostic to WAN transport technologies. SD-WAN provides dynamic, policy-based, application path selection across multiple WAN connections and supports service chaining for additional services such as WAN optimization and firewalls.

As organizations expand their operations across multiple branch locations, ensuring secure and streamlined connectivity becomes paramount. Deploying a secure branch network infrastructure involves complex configurations, which can be time-consuming and prone to configuration errors if not handled properly. However, organizations can overcome these challenges by leveraging the Cisco Secure Firewall Management Center (management center) and the Cisco Secure Firewall Threat Defense (threat defense) devices for a simplified and secure branch deployment.

In this guide, we explore the concept of simplifying secure branch deployment using a robust firewall solution. By integrating a secure firewall as a foundational component of the branch network architecture, organizations can establish a strong security baseline while simplifying the deployment process. This approach enables organizations to enforce unified security policies, optimize traffic routing, and ensure resilient connectivity.

Some of the SD-WAN capabilities supported on the Cisco Secure Firewall are:

- **Simplified management:**
  - SASE: Umbrella auto tunnel deployment
  - Dynamic VTI (DVTI) hub spoke topology simplification
- **Application awareness:**
  - Direct Internet Access (DIA) for public cloud and guest user
  - Policy based routing (PBR) using applications as a match criteria
  - Local tunnel ID support for Umbrella

- **Increased usable bandwidth:**
  - ECMP support for load balancing across multiple ISPs and VTIs
  - Application-based load balancing using PBR
- **High availability with near zero network downtime:**
  - Dual ISP configuration
  - Optimal path selection based on application-based interface monitoring.
- **Secure Elastic Connectivity:**
  - Route-based (VTI) VPN tunnels between headquarters (hub) and branches (spokes)
  - IPv4 and IPv6 BGP, IPv4 and IPv6 OSPF, and IPv4 EIGRP over VTI
  - DVTI hubs that support spokes with static or dynamic IP

Features

The following table lists some commonly used SD-WAN features:

Feature	Introduced in	More Information
SD-WAN Wizard	Release 7.6	Using SD-WAN Wizard for Secure Branch Network Deployment
Application monitoring using SD-WAN Summary dashboard	Release 7.4.1	SD-WAN Summary Dashboard
SD-WAN Summary Dashboard	Release 7.4	SD-WAN Summary Dashboard
Policy-based routing with user identity and SGTs	Release 7.4	Policy Based Routing
Policy-based routing using HTTP path monitoring	Release 7.4	Policy Based Routing
Loopback interface support for VTIs	Release 7.3	Configure Loopback Interfaces
Support for dynamic VTI (DVTI) with site-to-site VPN	Release 7.3	Dynamic VTI
Umbrella auto tunnel	Release 7.3	Deploy a SASE Tunnel on Umbrella
Support for IPv4 and IPv6 BGP, IPv4 and IPv6 OSPF, and IPv4 EIGRP for VTIs	Release 7.3	BGP OSPF EIGRP

Feature	Introduced in	More Information
Route-based site-to-site VPN with hub and spoke topology	Release 7.2	Create a Route-based Site-to-Site VPN
Policy-based routing with path monitoring	Release 7.2	Policy Based Routing
Site to Site VPN Monitoring Dashboard	Release 7.1	Monitoring the Site-to-Site VPNs
Direct Internet Access/Policy Based Routing	Release 7.1	Policy Based Routing
Equal-Cost-Multi-Path (ECMP) zone with WAN interfaces	Release 7.1	ECMP
ECMP zone with VTI interfaces	Release 7.1	ECMP
Backup VTI for route-based site-to-site VPN	Release 7.0	Route Traffic Through a Backup VTI Tunnel
Support for static VTI (SVTI) with site-to-site VPN	Release 6.7	Static VTI