Implementation Guides

https://campus.barracuda.com/doc/96025941/

Implementation Guides are manuals for the advanced user that provide extensive documentation on the concepts and workflow of the CloudGen Firewall and Control Center. Each guide concentrates on a specific topic and offers both a complete overview of the topic's available features as well as a suggested configuration path that includes limitations and issues to consider during implementation. The instructions are geared toward larger setups that use the advanced central management capabilities of the Control Center and the low-maintenance administration features it offers.

Available Implementation Guides

CloudGen Firewall in AWS Implementation Guide

This guide covers use cases and reference architectures for deploying a Barracuda CloudGen Firewall solution in AWS. After matching the use case to the reference architecture, the solutions are easily deployed with the provided CloudFormation templates. Also, take a look at the step-by-step instructions included to get more detailed information on a topic.

For more information, see Implementation Guide - CloudGen Firewall in AWS.

VPN Network with Static Routing Implementation Guide

This guide covers the configuration and concepts for creating a statically routed VPN network. The guide first goes over the process for configuring a large number of managed firewalls and points out what you need to keep in mind before undertaking such a project. Next, it discusses the tasks that you must complete for each individual unit and how to use the GTI editor to create a fully meshed VPN network. It also discusses when each firewall service should be used and include tips on how you can make the most of Barracuda Networks' advanced VPN features, such as SD-WAN or Dynamic Mesh VPN.

For more information, see Implementation Guide - VPN Network with Static Routing.

CloudGen Firewall in Microsoft Azure Implementation Guide

Microsoft Azure is one of the big players in the public cloud space offering IaaS and PaaS services to its customers. This guide covers how the Barracuda CloudGen Firewall plays a vital role in an Azure multi-tiered network design and how its connectivity and security features allow you to transparently and securely access and connect to your resources in the cloud. The Barracuda CloudGen Firewall connects and secures your applications in the public cloud. To manage a large number of firewalls, use the Barracuda Firewall Control Center, deployed either directly in Azure or on-premises.

For more information, see Implementation Guide - CloudGen Firewall in Azure.

How to Integrate a CloudGen Firewall with SCADAfence

This guide covers the integration of SCADAfence as a continuous network monitoring solution with the Barracuda CloudGen Firewall or Control Center. Offering API-based access with automated response mechanisms and adopting advanced Industrial IoT and OT technologies, SCADAfence provides more visibility and security for organizations and ensures flexibility in the actions performed.

For more information, see How to Integrate a CloudGen Firewall with SCADAfence.

How to Integrate Crosser Edge Analytics with the Barracuda Secure Connector

This guide covers the deployment of Crosser IoT Edge Streaming Analytics on the Barracuda Secure Connector in order to enable effective processing of useful data in an on-premises or cloud analytics platform. Deployed as a container, the solution allows collected data to be aggregated, combined, and prefiltered to reduce the cost for storage and intermittent transmission.

For more information, see How to Integrate Crosser Edge Analytics with the Barracuda Secure Connector.

How to Enable Filebeat Stream to a Logstash Pipeline

This guide covers the configuration of Filebeat log data streaming from Barracuda Firewall Insights to a Logstash server in order to gather information on firewall activity, threat logs, and information related to network, version, and location of managed firewall units.

For more information, see How to Enable Filebeat Stream to a Logstash Pipeline.

How to Enable Integration with Barracuda XDR

Barracuda XDR detects threats with a managed XDR platform, backed by a 24×7 Security Operations Center (SOC) to streamline response to incidents reducing the potential damage of attacks. Customer data is stored in the respective region where the customer is located. Any transfer of customer data outside the regions will be done in compliance with the GDPR and applicable local privacy laws. Barracuda XDR supports TLS protocol to transfer data from customer sensors to the data lake in AWS.

For more information, see How to Enable Integration with Barracuda XDR.

How to Enable Integration with Nozomi Networks

This guide covers the integration of the Barracuda CloudGen Firewall with Nozomi Networks, which extends the capability of a passive approach of monitoring and anomaly detection to an automated active action that blocks suspicious traffic.

For more information, see How to Integrate the Barracuda CloudGen Firewall with Nozomi Networks.

How to Integrate the Barracuda CloudGen Firewall with Rhebo

Rhebo is a network monitoring solution for industrial control systems (ICS) and operational technology (OT) networks. It uses real-time monitoring and machine learning algorithms to detect anomalies and cyber threats, such as malware and unauthorized access attempts. The solution also provides detailed insights into network activity, including data on protocols, devices, and communication patterns. This allows organizations to improve the security and reliability of their OT networks and protect against potential disruptions to critical infrastructure.

For more information, see How to Integrate the Barracuda CloudGen Firewall with Rhebo.

How to Connect the Barracuda CloudGen Firewall to the Teridion Network

Teridion is a cloud-based network service that leverages the power of the cloud to optimize Internet traffic and provide faster, more reliable connectivity for businesses, applications and other services. At its core, Teridion uses a global network of endpoints and advanced routing technologies to intelligently route traffic across the Internet, avoiding congestion and bottlenecks to ensure optimal performance.

For more information, see How to Connect the Barracuda CloudGen Firewall to the Teridion Network via IPSec and How to Connect the Barracuda CloudGen Firewall to Teridion via GRE Tunnel.