

JUNIPER-CORERO DDoS PROTECTION IMPLEMENTATION SERVICE DATASHEET

Service Overview

The Juniper-Corero DDoS Protection Implementation Service is specifically designed to support initial deployment of the joint Juniper-Corero DDoS protection solution. As distributed denial of service (DDoS) attacks grow in frequency, magnitude, and sophistication, traditional defenses such as out-of-band scrubbing centers and manual interventions prove woefully inadequate and cost-prohibitive. The joint Juniper-Corero solution is highly effective, automated, and scales to multi-terabit capacity at a much lower cost than competitive offerings.

Service Description

Juniper Networks and Corero Network Security have partnered to develop a revolutionary DDoS solution that self-heals the network through rapid identification, precise decision making, automated mitigation at strategic places in the network, and continuous monitoring. Consisting of Corero SmartWall Threat Defense Director (TDD) and Juniper Networks® MX Series Universal Routing Platforms, the solution filters out DDoS attack traffic at the edge of your network.

The Juniper Networks-Corero DDoS Protection Implementation Service gives your organization access to Juniper® Professional Services security experts who will deploy the joint solution. Built on a reference architecture, this service provides Juniper subject matter experts who will analyze your current network and provide recommendations. The service package also includes Professional Services work covering the installation and setup of the Corero SmartWall TDD product components, including system configuration, initial tuning, and an add-on option for TDD self-service portal implementation.

Architecture and Key Components

The Juniper-Corero DDoS protection solution includes MX Series edge devices and a Corero SmartWall Threat Defense Director (TDD) to protect your environment from DDoS-based volumetric attacks. The TDD works with the MX Series routers to filter out DDoS attack traffic at the network edge.

The Juniper-Corero DDoS protection solution consists of the following components:

- SmartWall Threat Defense Director (TDD), which is a bundle of the following virtual applications:
 - The SmartWall Network Threat Defense Virtual Edition (vNTD), which is the detection engine for the SmartWall TDD. It detects DDoS attack traffic in mirrored samples sent from the edge routers.
 - The SmartWall Central Management Server Virtual Edition (vCMS), which controls the vNTD, enabling you to configure the attack mitigation policy used to distinguish attack traffic from normal network traffic.
 - The SmartWall SecureWatch Analytics Virtual Edition (vSWA), which receives information from the vNTD (via the vCMS) to identify DDoS attacks currently active against your network. The vSWA application then sends firewall filter commands to the router to screen attack traffic as it arrives at the router. The vSWA application also displays both real-time and historical statistics that enable you to analyze attacks on your network.

- Remote Devices:
 - The MX Series routers, deployed at the edge of the network being protected, send sampled traffic to the vNTD.
 - They are directed by vSWA to apply firewall filters to block DDoS attack traffic.

Figure 1 depicts the main functional blocks and logical interconnection points of this joint solution.

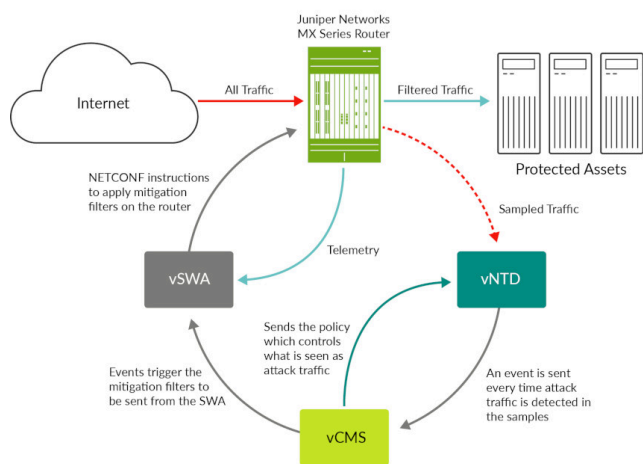


Figure 1: Juniper-Corero DDoS protection solution

Service Deliverables

TDD Solution Workshop

Juniper Networks will provide a consulting style workshop to review and interactively discuss the technical aspects of the Juniper-Corero DDoS protection solution. The workshop includes high-level discussions on DDoS protections and the solution approach using TDD, reference architecture, and how the TDD integrates with the MX Series routers. The workshop provides a recommended deployment approach and guidance toward future expansion.

TDD Base Implementation

Juniper Networks will review the existing design with your team, verify requirements, analyze the data points, and provide a specific design document. Utilizing the details from the design document, Juniper will give you a specific plan for deploying the Juniper-Corero DDoS protection solution in your environment. Juniper will work with your team to deploy the solution by following the plan. After successful deployment, Juniper will review the solution components, provide a knowledge transfer workshop on the deployed solution, and tune the predefined rules, if needed.

TDD Portal Implementation (Optional Add-On)

Upon conclusion of the TDD base implementation and any initial tuning, Juniper will provide an optional service add-on for technical assistance deploying the TDD SmartWall Service Portal (SSP). This includes initiation of the SSP add-on Web application, onboard testing, assigning DDoS protection service levels, and viewing attack dashboards.

Milestone	Feature and Descriptions	Benefit
TDD Solution Workshop	Juniper will conduct a workshop to review the customer's current design. Based on the solution reference architecture, key solution requirements will be identified with details on how the reference solution with TDD can be incorporated into the network.	The customer will receive a recommendation document with localized details of the project and placement of the solution with TDD based on the customer's requirements prepared by Juniper.
TDD Base Implementation	Based on the localized reference design, Juniper will localize the standard implementation guide and prepare a deployment checklist. Following this guide, Juniper consultants will assist in deploying the solution.	Juniper will provide the customer with a specific plan for deploying the joint Juniper-Corero DDoS protection solution. Execution of the steps will be documented in the plan by the Juniper consultant. Juniper will work with the customer to review the components of the solution and fine-tune the predefined rules. Juniper will also provide a knowledge transfer workshop on the deployed solution as described in the design document.
TDD Portal Implementation (optional)	Juniper will provide technical assistance when deploying the TDD SSP. This includes the initiation of the SSP add-on Web application, onboarding the test customer, assigning DDoS protection service levels, and viewing attack dashboards.	The TDD Service Portal is an optional component that enables customers to offer Juniper-Corero DDoS protection as a managed service. The Service Portal uses traffic data from TDD and displays the information in easy-to-read dashboards and reports. The Juniper consultant will help customers create reports to highlight the value they receive from the DDoS protection service, based on the number and size of the attacks.

Juniper Service and Support

Juniper ensures operational excellence by optimizing the network to maintain required levels of performance, reliability, and availability. For more details, please visit <https://www.juniper.net/us/en/products.html>.

Ordering Information

To order the Juniper-Corero DDoS Protection Implementation Service, or for additional information, please contact your Juniper Account Manager.

Exclusion

The scope of this service is for Juniper-Corero DDoS Protection Implementation Service only and does not include separately sold assessment, design, or deployment services. If you require additional services from your Juniper Professional Services consultant, please contact your Juniper Account Manager.

About Juniper Networks

At Juniper Networks, we are dedicated to dramatically simplifying network operations and driving superior experiences for end users. Our solutions deliver industry-leading insight, automation, security, and AI to drive real business results. We believe that powering connections will bring us closer together while empowering us all to solve the world's greatest challenges of well-being, sustainability, and equality.

Corporate and Sales Headquarters

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA

Phone: 888.JUNIPER (888.586.4737)

or +1.408.745.2000

www.juniper.net

APAC and EMEA Headquarters

Juniper Networks International B.V.
Boeing Avenue 240 1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands

Phone: +31.207.125.700

