



Service Description: Advanced Services – Fixed Price

Check Point to ASA 5510 Firewall Configuration Migration Service (ASF-CORE-ASA10-MIG)

This document describes Advanced Services Fixed Price: Check Point to ASA Firewall Configuration Migration Service

Related Documents: This document should be read in conjunction with the following documents also posted at www.cisco.com/go/servicedescriptions/: (1) Glossary of Terms; (2) List of Services Not Covered. All capitalized terms in this description have the meaning ascribed to them in the Glossary of Terms.

Direct Sale from Cisco. If you have purchased these Services directly from Cisco for your own internal use, this document is incorporated into your Master Services Agreement, Advanced Services Agreement, or other services agreement covering the purchase of Advanced Services-based services with Cisco ("Master Agreement"). If no such Master Agreement exists, then this Service Description will be governed by the terms and conditions set forth in the Terms & Conditions Agreement posted at <http://www.cisco.com/legal/advancedservices.html>. If you have purchased these Services directly from Cisco for resale purposes, this document is incorporated into your System Integrator Agreement or other services agreement covering the resale of Advanced Services ("Master Resale Agreement"). If the Master Resale Agreement does not contain the terms for the Purchase and Resale of Cisco Advanced Services or equivalent terms and conditions, then this Service Description will be governed by the terms and conditions of the Master Resale Agreement and those terms and conditions set forth in the SOW Resale Terms & Conditions Agreement posted at: <http://www.cisco.com/legal/advancedservices.html>. For purposes of the SOW Resale Terms and Conditions this Service Description shall be deemed as a Statement of Work ("SOW"). In the event of a conflict between this Service Description and the Master Agreement or equivalent services exhibit or agreement, this Service Description shall govern.

Sale via Cisco Authorized Reseller. If you have purchased these Services through a Cisco Authorized Reseller, this document is for description purposes only; is not a contract between you and Cisco. The contract, if any, governing the provision of this Service will be the one between you and your Cisco Authorized Reseller. Your Cisco Authorized Reseller should provide this document to you, or you can obtain a copy of this and other Cisco service descriptions at www.cisco.com/go/servicedescriptions/.

Check Point to ASA Firewall Configuration Migration Service

Service Summary

The Check Point to Cisco ASA 5510 Firewall Configuration Migration Service provides remote configuration migration services to Customer. Cisco will convert the firewall policy for one (1) Customer selected Check Point or Juniper firewall to one (1) Cisco ASA 5510 firewall configuration ("Services"). In case there are virtualized environments (either Check Point, Juniper, or Cisco ASA), the Services will include converting policies for one (1) context, limited to fifty (50) rules, five hundred (500) objects, and three (3) interfaces.

The Services may include firewall policy conversion from one of the following Check Point or Juniper platforms:

- Check Point Firewall-1®, SmartCenter (v 3.0 and up)
- Check Point VSX® (all versions)
- Check Point Security Gateway VE® (all versions)
- Juniper NetScreen® Series (v 5.0 and up)
- Juniper Network and Security Manager® (NSM) (v2008.1 and up)
- Juniper SRX® Series (requires NSM v2001.1 and up)

to one Cisco Adaptive Security Appliance (ASA) 5510 with 7.x or 8.x software versions

Location of Services

Services are delivered remotely to Customer.

Check Point Firewall Information Gathering

Cisco Responsibilities

- Review for completeness the following Customer-provided information to use as input for the firewall configuration migration:
 - existing code versions and configuration files with policy rule-sets of appropriate Check Point or Juniper firewall;
 - addressing schemes and interface configurations;
 - applications and protocols supported through the Check Point or Juniper firewall;
 - naming conventions, policy controls and workflow.

Customer Responsibilities

- Provide the following:
 - existing code versions and configuration files with policy rule-sets of appropriate Check Point or Juniper firewall;
 - addressing schemes and interface configurations;
 - applications and protocols supported through the Check Point or Juniper firewall;
 - naming conventions, policy controls and workflow

Firewall Policy Conversion

Cisco Responsibilities

- Convert the existing Check Point or Juniper firewall configuration and security policy rule-sets into a Cisco ASA 5510 configuration file and security policies rule-sets using the Customer-provided Check Point or Juniper configuration information and the ASA Migration tool.
- Compare the Cisco ASA 5510 firewall configuration file and security policies rule-sets to the Customer's original Check Point or Juniper firewall configurations to verify accuracy.
- Review with Customer the Cisco ASA 5510 configuration file and security policies rule-sets for understanding and knowledge transfer.

Customer Responsibilities

- Review the Cisco ASA 5510 configuration file and security policies rule-sets with Cisco.

General Customer Responsibilities

- All information (such as but not limited to: designs, topologies, requirements) provided by Customer is assumed to be up-to-date and valid for the Customer's current environment. Cisco Services are based upon information provided to Cisco by Customer at the time of the Services.
- Customer acknowledges that the completion of Services is dependent upon Customer meeting its responsibilities as indicated herein.
- Identify Customer's personnel and define their roles in participation of the Services. Such personnel may include but is not limited to: architecture design and planning engineers, and network engineers.
- Ensure Customer's personnel are available to participate during the course of the Services to provide information and to participate in scheduled information gathering sessions, interviews, meetings and conference calls.
- Services provided by Cisco comprise technical advice, assistance and guidance only.
- Customer expressly understands and agrees that the Services shall take place and complete within ninety (90) calendar days from issuing a Purchase Order to Cisco for the Services herein.

Invoicing and Completion

Invoicing

Services will be invoiced upon completion of the Services.

Completion of Services

Cisco will provide written notification upon completion of the Services to Authorized Channel. The Authorized Channel shall within five (5) Business Days of receipt of such notification provide written acknowledgement of Cisco's completion of the Services. Authorized Channel's failure to acknowledge completion of the Services or to provide reasons for rejection of the Services within the five (5) Business Day period signifies Authorized Channel's acceptance of completion of the Services in accordance with this Service Description.