

# **Edge Firewall ATP - Geo-IP**

VeloCloud Products

Exported on 11/20/2024

# Table of Contents

1	PRD SIGN-OFF .....	3
2	1.0 Feature Description .....	4
3	2.0 Objective.....	5
4	3.0 Use Cases .....	6
5	3.1 Enhanced Firewall Services (EFS) License .....	7
6	4.0 Assumptions .....	8
7	5.0 Impact.....	9
8	6.0 Management Plane Requirements .....	10
9	6.1 Data Plane Requirements.....	17
10	6.2 Hardware Requirements .....	18
11	7.0 Operational Readiness .....	19
12	8.0 Supportability .....	20
	12.1 Alerts.....	20
	12.2 Logging and Events .....	20
	12.3 Remote Diagnostics.....	20
	12.4 Visibility / Troubleshooting tools .....	20
13	10.0 Performance and Scale Requirements .....	21
14	11.0 User Story.....	22
15	12.0 Open Questions .....	23
16	13.0 Out of Scope .....	24

# 1 PRD SIGN-OFF

Target Release	APEROL
Sign-Off Date	
Epic	<a href="#">VLENG-122596</a> <sup>1</sup>
Feature Size	M
PRD Status	IN REVIEW
PM Owner	@Sathya Thammanur
Architect	@Aditya Agarwal
MP Owner	@Preethi Nandakumar
DP Owner	@Gobu Ezhumalai
QA Owner	@Preethi Nandakumar
UX Owner	@Ritesh Tiwari

<sup>1</sup> <https://jira.eng.vmware.com/browse/VLENG-122596>

## 2

### 1.0 Feature Description

Geo-IP is an advanced protection capability on edge FW that provides the ability to:

- Block or allow access to traffic flows at edge based on geolocation or country to meet compliance requirements
- Allow edge firewall policy rule creation applicable to specified countries or region

## 3 2.0 Objective

Currently, VCE FW provides stateful inspection along with application identification without additional ATP security features. While the stateful FW of VCE provides security, it is not adequate and creates a gap in providing ATP security integrated natively with SDWAN. Edge Enhanced Firewall services (EFS) goal is to address these security gaps and offer advanced threat protection natively on the edge in conjunction with SDWAN. The solution is a significant initiative both in terms of customer retention (SD-WAN customers looking for integrated advanced security solutions) and market expansion. To this end, EFS was launched starting with IDS/IPS in 5.2 and continuing up to URL Filtering and Malicious IP Filtering in 6.0 releases. EFS will expand to include Geo-IP as part of the advanced security offer.

## 4 3.0 Use Cases

Please list out the use cases. Examples below:

#	User Story
1	A security admin must be able to set firewall access restrictions based on specific geo locations (country)
2	A security admin must be able to see geo location of IP addresses in logs
3	A security admin must be able to visualize in dashboard the list of geo locations blocked based on access rule restrictions configured
4	A security admin must be able to create reusable GeoIP settings that is used across multiple firewall policies

## 5 3.1 Enhanced Firewall Services (EFS) License

Geo-IP will be included as part of the EFS add-on license that currently supports IDS/IPS, URL Filtering and Malicious IP Filtering. EFS add-on license can be used with any of the available SD-WAN editions (Standard, Enterprise, Premium).

## 6 4.0 Assumptions

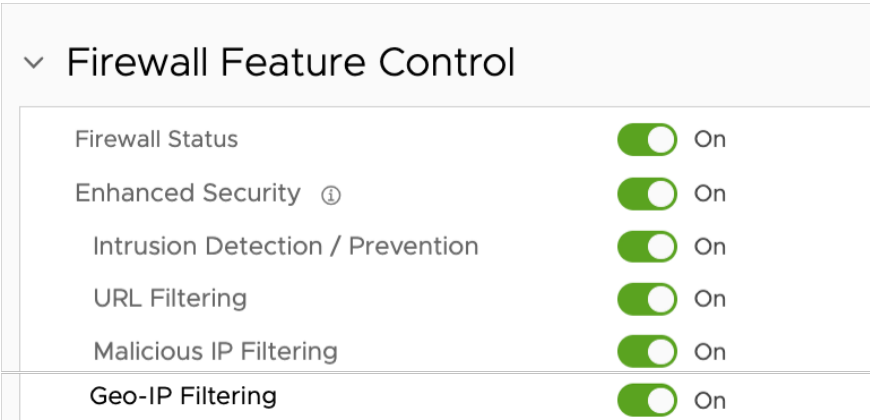



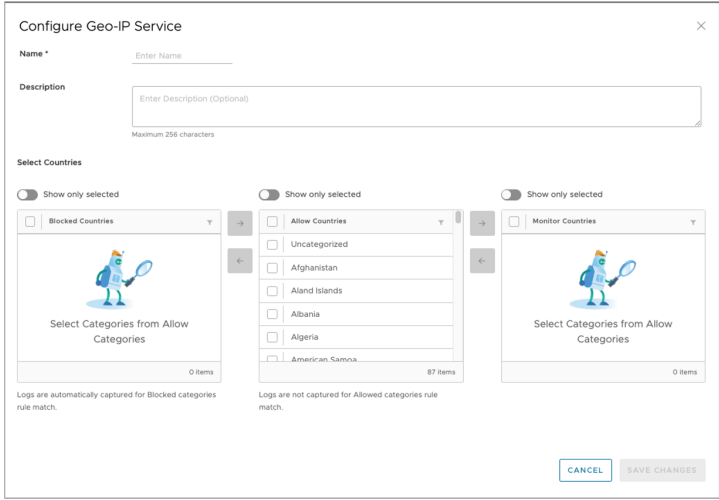
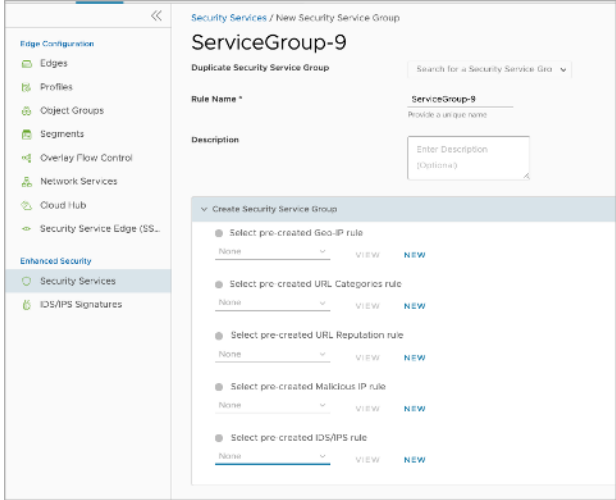
## 7 5.0 Impact

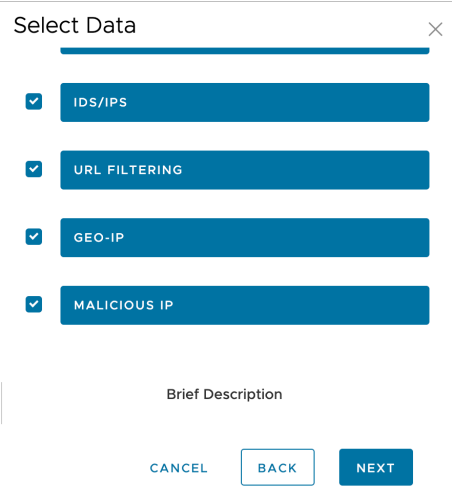
Impact	Response	Comments
DP Documentation	<input checked="" type="checkbox"/> User Guide <input checked="" type="checkbox"/> DP Monitoring <input type="checkbox"/> No Doc Required	
MP Documentation	<input checked="" type="checkbox"/> User Guide <input checked="" type="checkbox"/> MP Monitoring <input type="checkbox"/> No Doc Required	
Platform Documentation	<input checked="" type="checkbox"/> User Guide <input type="checkbox"/> No Doc Required	
Feature Flag	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	Uses existing Enhanced Firewall Services Feature Access
TechOps Impact (Architecture Changes?)	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Not Sure	
UI Impact	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Not Sure	
UX Impact	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Not Sure	<p>Figma UX Workflow:</p> <div>  <p>Sorry, the widget is not supported in this export. But you can reach it using the following URL:</p> <p><a href="https://www.figma.com/design/udG3bfEiaJYuUD5z0hZAVf/Edge-Firewall-ATP?node-id=6551-92521&amp;t=71NVPWahQPaoFpfd-1">https://www.figma.com/design/udG3bfEiaJYuUD5z0hZAVf/Edge-Firewall-ATP?node-id=6551-92521&amp;t=71NVPWahQPaoFpfd-1</a></p> </div>

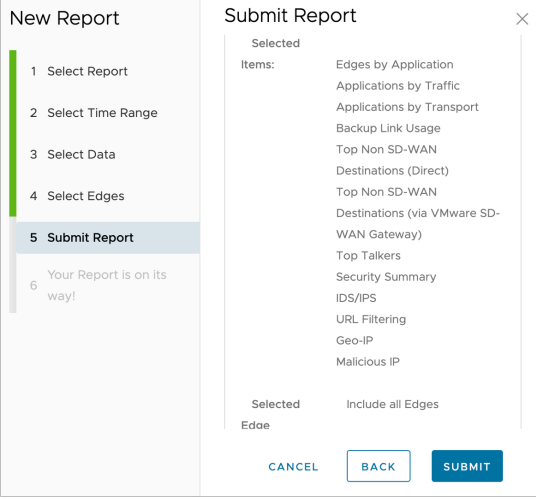
## 8

## 6.0 Management Plane Requirements

#	Requirements	Importance	ETA	Jira Issue
MP 1.1	Geo-IP will be included as part of the EFS offer and hence should be controlled by the Enhanced Firewall Services Feature Access flag in the customer configuration.	HIGH	APE ROL	
MP 1.2	<p>Add Geo-IP as a new security service under Enhanced Security Feature Control:</p> 	HIGH	APE ROL	
MP 1.3	<p>Add Geo-IP as a new security service in the Security Services section</p>  <p>Engine ordering listed will follow Figma specifications as provided by the UX team.</p>	HIGH	APE ROL	

#	Requirements	Importance	ETA	Jira Issue
MP 1.4	<p>Provide users ability to create Geo-IP rules under Security Services section. Similar to other Security services, an Add Rule under Geo-IP will open up the following pop up to configure for Blocked, Allow, Monitor countries</p>  <p>Use Figma from UX team for the actual screenshot/text for Geo-IP configuration</p>	HIGH	APE ROL	
MP 1.5	<p>Add Geo-IP as a selectable configuration for Security Services Group creation workflow. Use Figma from UX team for the actual screenshot/ configuration.</p> 	HIGH	APE ROL	

#	Requirements	Importance	ETA	Jira Issue
<a href="#">MP 1.6</a>	Security Services Groups tool tip must include Geo-IP rule configuration as part of the Firewall rules displayed in the Firewall Rules table	HIGH	APE ROL	
<a href="#">MP 1.7</a>	<b>Backwards Compatibility</b> VECO must ensure configurations from releases 4.x/5.x/6.x can be seamlessly migrated with the addition of Geo-IP.	HIGH	APE ROL	
<b>Reporting</b>				
<a href="#">MP 1.8</a>	Add Geo-IP to "Select Data" in the "items" and "Brief Descriptions" areas in the "New Report" modal. 	HIGH	APE ROL	

#	Requirements	Importance	ETA	Jira Issue
MP 1.9	<p><i>Under "Report Summary" in New Report → Submit Report should include Geo-IP if selected.</i></p> 	HIGH	APRIL	

#	Requirements	Importance	ETA	Jira Issue																										
MP 1.10	<p>PDF Report - Use Figma for the actual screenshot for the widget to add to the report.</p> <p>a. Security summary must include Geo-IP if selected.</p> <p>b. Table of reporting edges must include Geo-IP</p> <p>c. Geo-IP Section content:</p> <p><i>Top Edges (up to a max of 10) by Action</i></p> <table><tr><th>Edge Name</th><th>Blocked</th><th>Allowed</th><th>Monitored</th><th>Total Count</th></tr><tr><td>branch_edge</td><td>20</td><td>50</td><td>10</td><td>80</td></tr></table> <p><i>Top Geo-IP Destinations by IP</i></p> <table><tr><th>IP</th><th>Blocked</th><th>Monitored</th><th>Total Count</th></tr><tr><td>1.2.3.4</td><td></td><td></td><td></td></tr></table> <p><i>Top Geo-IP Destinations - Country</i></p> <table><tr><th>Country</th><th>Blocked</th><th>Monitored</th><th>Total Count</th></tr><tr><td>Russia</td><td></td><td></td><td></td></tr></table>	Edge Name	Blocked	Allowed	Monitored	Total Count	branch_edge	20	50	10	80	IP	Blocked	Monitored	Total Count	1.2.3.4				Country	Blocked	Monitored	Total Count	Russia				HIGH	APE ROL	
Edge Name	Blocked	Allowed	Monitored	Total Count																										
branch_edge	20	50	10	80																										
IP	Blocked	Monitored	Total Count																											
1.2.3.4																														
Country	Blocked	Monitored	Total Count																											
Russia																														

#	Requirements	Importance	ETA	Jira Issue
MP 1.1 1	<p>CSV Report -</p> <ol style="list-style-type: none"> <li><i>List all edges impacted by Geo-IP</i>  Name of CSV File: <i>GeoIPStats.csv</i>  Column headers:  <i>edge_name, num_of_blocked, num_of_monitored, total_count</i></li> <li><i>List all Geo-IP Destinations by IP</i>  Name of CSV File: <i>topGeoIPDestinationsByIP.csv</i>  Column headers:  <i>destination_ip, num_of_blocked, num_of_monitored, total_count</i></li> <li><i>List all Geo IP Destinations by Country</i>  Name of CSV File: <i>topGeoIPDestinationsByCountry.csv</i>  Column headers:  <i>destination_country, num_of_blocked, num_of_monitored, total_count</i></li> </ol>	HIGH	APE ROL	
	<b>Monitoring</b>			
MP 1.1 2	<p><b>Security Overview</b></p> <ol style="list-style-type: none"> <li>Add Geo-IP Summary to Security Overview with the following information: <ul style="list-style-type: none"> <li>Geo-IP w/ Total Actions (Aggregate of all edges data in Enterprise View, Individual Edge data in Edge View)</li> <li>Top Countries donut with Actions listed across Blocked, Allowed, Monitor action types</li> </ul> </li> <li>Add Geo-IP Tab to the list of engine data</li> </ol> <p>Use Figma for actual UX representation</p>	HIGH	APE ROL	

#	Requirements	Importance	ETA	Jira Issue
MP 1.1 3	<b>Geo-IP Section</b> <ol style="list-style-type: none"> <li>Start with Geo-IP Summary as: <ol style="list-style-type: none"> <li>Geo-IP w/ Total Actions (Aggregate of all edges data in Enterprise View, Individual Edge data in Edge View)</li> <li>Top Countries donut with Actions listed across Blocked, Allowed, Monitor action types</li> </ol> </li> <li>Include the following widgets <ol style="list-style-type: none"> <li>Top Countries By Actions</li> <li>Top Edges by Actions (For Enterprise)</li> <li>Top Sources By Actions (For Edge)</li> </ol> </li> </ol>	HIGH	APERO	



## 9 6.1 Data Plane Requirements

#	Requirements	Importance	ETA	Jira Issue
<a href="#">D</a> <a href="#">P</a> <a href="#">1.1</a>	Geo-IP engine must action on a flow when the engine is enabled in Firewall Feature Control.	<b>HIGH</b>	<b>APERO</b>	
<a href="#">D</a> <a href="#">P</a> <a href="#">1.2</a>	<b>Geo-IP Policy Actions</b> Based on the user classification of countries, the edge platforms takes one of the below actions <ul style="list-style-type: none"> <li>• <b>ALLOW</b>: Flow allowed to destined country and no further action taken</li> <li>• <b>MONITOR</b>: Flow is allowed to destined country and logged</li> <li>• <b>BLOCK</b>: Flow is blocked if destination country falls into the BLOCK configuration of Geo-IP settings</li> </ul>	<b>HIGH</b>	<b>APERO</b>	
<a href="#">D</a> <a href="#">P</a> <a href="#">1.3</a>	<b>Unknown Country</b> Apart from pre-defined countries (1:1 mapping with Maxmind countries), a flow destination with no country mapping available from the DB lookup will be blocked by default and allowed only if user configures "Unknown Country" checkbox.	<b>HIGH</b>	<b>APERO</b>	
<a href="#">D</a> <a href="#">P</a> <a href="#">1.4</a>	<b>Geo-IP Database</b> Geo-IP engine uses a local country database to do lookup on destination IP for country match. Database is obtained via VECO using the same infrastructure that is currently used to download IDPS signature bundle.	<b>HIGH</b>	<b>APERO</b>	
<a href="#">D</a> <a href="#">P</a> <a href="#">1.5</a>	<b>Geo-IP Maxmind SDK</b> IP to country match lookup in the local edge database is done via AP from Maxmind. Dataplane integrates uses Maxmind SDK for doing country lookup.	<b>HIGH</b>	<b>APERO</b>	

## 10 6.2 Hardware Requirements

#	Requirements	Importance	ETA	Jira Issue

## 11 7.0 Operational Readiness

*Describes the impact to TechOps as well as any requirements for license enforcement, special documentation or cross BU dependencies. Also, note any considerations on the ability to order (e.g. if new SKUs are needed).*

## 12 8.0 Supportability

*Call out any supportability requirements for this feature as well as any requirements for alerts, logging and events, remote diagnostics, and visibility/troubleshooting tools.*

### 12.1 Alerts

*Describes any new alerts that should be added.*

### 12.2 Logging and Events

*Describes any logging requirements or events that should be generated associated with this feature.*

### 12.3 Remote Diagnostics

*Call out any new additions or changes to the remote diagnostics page.*

### 12.4 Visibility / Troubleshooting tools

*Call out any requirements for Visibility and troubleshooting tools.*

## 9.0 Security Requirements

## 13 10.0 Performance and Scale Requirements

Platform	IMIX (400B) Performance (Mbps)	Max Concurrent Session	Max CPS	Max CPS with Logging
Edge 510				
Edge 510- LTE				
Edge 520				
Edge 520v				
Edge 540				
Edge 840				
Edge 3400				
Edge 2000				
Edge 3800				
Edge 620				
Edge 640				
Edge 680				

## 14 11.0 User Story

Please work with Development Team to determine/define the user stories for the feature of interest if needed.

#	User Story	Priority
1	As a (persona), I want (state the intent), so that (the benefit/ what is expected to achieve.  Example: As a power user, I want to specify files or folders to backup based on file size, date created and date modified, so that I can better manage data records.	
2		
3		

15

## 12.0 Open Questions

Question	Answer	Date Answered

## 16 13.0 Out of Scope