Generate FMC Reports for VPN Users

Contents

troduction
rerequisites
Requirements
Components Used
ackground Information
onfigure
Configurations
enerate Report
Procedure
<u>esult</u>

Introduction

This document describes how to generate reports which provide at-a-glance views of consolidated information about VPN users, including the current status of users, device types, client OS, client applications, and duration of connections on the Firepower Management Center.

Prerequisites

Requirements

Cisco recommends that you have the knowledge of these topics:

- Cisco Firepower Threat Defence (FTD)
- Cisco Firepower Management Center (FMC)
- Anyconnect Secure Mobility Client

Components Used

The information in this document is based on these software versions:

- Cisco FMC for VMware with version 7.x
- AnyConnect Secure Mobility Client 4.x

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

The Firepower System provides a flexible reporting system that allows you to quickly and easily generate reports on your Firepower Management Center. You can also design your custom reports from scratch. A report is a document file formatted in PDF, HTML, or CSV with the content you want to communicate

while a report template specifies the data searches and formats for the report and its sections. The Firepower System includes a powerful report designer that automates the design of report templates. You can include field parameters like authentication type, connection duration and so on in a template to expand its usefulness.

Remote access VPNs provide secure connections for remote users, such as mobile users or telecommuters. Monitoring these connections provides important indicators of connection and user session performance at a glance. You must be an Admin user in a leaf domain to perform this task. The Firepower System monitoring capabilities enable you to determine quickly whether remote access VPN problems exist and you can then apply this knowledge and use your network management tools to reduce or eliminate problems for your network and users.

Configure

Configurations

Step 1. Select Overview > Dashboards > Reporting > Report Templates and click on Create Report Template as shown in the image.

CISCO Firepower Management Center Overview / Reporting / Report Templates	Overview Analysis Policies	s Devices Objects	AMP Intelligence	Deptoy Q 🗳 🌣 😡 admin
Reports Report Templates	Dashboards Dashboard	Summary Intrusion Event Statistics	-	
	Management	Intrusion Event Performance		Create Report Template
Risk Report Templates	Reporting	Intrusion Event Graphs Discovery Statistics		
Advanced Malware Risk Report		Discovery Performance	1:05:21 Imin"	日本のノ主
Attacks Risk Report		Connection Summary	:05:21 min*	■ % C × *
Network Risk Report		2023-10-31 Modified by	11 08:05:21 y "admin"	0 h C / P
Templates		Last Modifie	ed	
Attack Report: \$ <attack sid=""></attack>		2023-04-05 Modified by	i5 07:28:40 y "admin"	日期にノ東
Files Report		2023-04-05 Modified by	/5 07:28:41 y "admin"	8 % C / ¥
FirePOWER Report: \$ <customer name=""></customer>		2023-04-05 Modified by	15 07:28:41 y "admin"	8 % C / ¥
Host Report: \$ <host></host>		2023-04-05 Modified by	/5 07:28:41 y "admin"	8 % C / ¥
Mahware Report		2023-04-05 Modified by	/5 07:28:41 y "admin"	8 % C / 9
Report of User Activity		2023-10-17 Modified by	7 03:17:13 y "admin"	8 % C / ¥
Report of VPN Troubleshooting		2023-10-12 Modified by	2 02:29:58 y "admin"	8 % C / ¥
TZ-VPN-Report		2023-10-17 Modified by	7 05:22:24 y "admin"	8 % C / \$
User Report: \$ <user></user>		2023-04-05 Modified by	/5 07:28:41 y "admin"	8 % C / ¥
VPN User Activity Report		2023-10-31 Modified by	11 08:05:17 y "admin"	8 % C / ¥
new-test-vpn		2023-10-31 Modified by	11 07:37:46 y "admin"	8 % C / ¥

Create Report Template

Step 2. Enter a name for the template in the Report Title field as shown in the image.

Gisco Firepower Management Center Overview / Reporting / Report Template Designer	Overview	Analysis	Policies	Devices	Objects	AMP	Intelligence	Deploy Q 🧳 🌣 🔞 admin 🔻
Reports Report Templates								
Report Title								Generate Advanced Save
Report Sections								■K¢m∎TE9
				No Sect	ions			

Report Title

Step 3. Select Add Table View from the set of views available on the right side. You can also use charts such as bar charts, line charts, pie charts, and so on as per your requirements.

Firepower Management Center Overview / Reporting / Report Template Designer	Overview	Analysis	Policies	Devices	Objects	AMP	Intelligence	Deplo	уq	69 3	¢ 0	admin 🔻
Reports Report Templates												
Report Title VPN User Activity Report + Report Sections								Gener	ate	Adva	nced	Save
				No Sect	ions							

Add Table View

Step 4. Enter a title for the section in the Report Section Title field. Here, Table View of Events and Users table views have been added as shown in the image.

Firepower Management (Overview / Reporting / Report Temp	enter Overview Ar te Designer	nalysis Policies	Devices Objects	AMP	Intelligence	Deploy Q 🧳	¢ 0	admin •
Reports Report Templates								
Report Title VPN User Activity Report +						Generate Adva	nced	Save
Report Sections						ы м е	пв	твы
Table View of Events								+ 🗑
Table User Activity	•				Section Description \$ <time window="">\$<constraints></constraints></time>			
Preset None	*				Time Window 📄 Inherit Time Window 🛛 🖉 Last hour			
Format 🔟 🕑 🚺					Maximum Results 10000			
Search None	• /							
Fields Time, Event, U	ername, Realm, Di: 🖉							Preview
🖩 🔻 Users								+ ¥
Table Liver Activity					Section Description S <time windowsscconstraints=""></time>			
Preset None	•				Time Window Inherit Time Window Last hour			
Format 🔟 🗠 🕼					Maximum Results 10000			
Search None	× /							
Fields Count, Userna	ne 🖌							
							1	Preview

Title for Report Section

Step 5. Select User Activity under the Table drop-down menu as shown in the image.

Firepower Ma	anagement Center g / Report Template Designer Overview	Analysis	Policies	Devices	Objects	AMP	Intelligence	Deploy Q 💕 🌣 🔕 admi
Reports Report Temp	lates							
Report Title								Generate Advanced Saw
VPN User Activity Report	+							
Report Sections								M M C II B T E
Table View of Events								+ i
Table	Llear Activity						Section Description SzTime Windows SzConstraintes	
Tuble	Intrusion Events with Destination Criticality	-						
Preset	Intrusion Events with Source Criticality						Time Window 🗌 Inherit Time Window 🔮 Last hour	
Format	Malware Events						Maximum Results 10000	
	Remediation Status							
Search	Rule Update Import Log	r						
Fields	SSL Statistics							
Thomas	Scan Results Security Intelligence Events							
	Security Intelligence Statistics							Preview
🖬 🔻 Users	Servers							+ i
	Third-Party Vulnerabilities							
Table	URL Category Statistics						Section Description ScTime WindowsScConstraints>	
	User Activity						Contraction of the tribution of contracting	
Preset	User Indications of Compromise						Time Window 🔄 Inherit Time Window 🔮 Last hour	
5 mm	User Statistics						Mariana Daraka (10000	
Format	Users VDN Troubleshooting						Maximum Results	
Search	Vulnerabilities	1						
Fields	Count, Username							
								Preview

Select User Activity

Step 6. Choose a Preset value if required, otherwise, keep it as None .

Gisco Firepower Management Center Overview / Reporting / Report Template Designer	Overview	Analysis	Policies	Devices	Objects	AMP	Intelligence	Deploy Q 💕 🌣 g admi
Reports Report Templates								
Report Title								Generate Advanced Sav
VPN User Activity Report +								
Report Sections								M M C M B T E
Table View of Events								+ i
Table User Activity	•						Section Description \$ <time window="">\$<constraints></constraints></time>	
Propert Name	-						Time Window 🖂 Jaharit Time Window 🌨 Last hour	
Preset None	÷	193					Time window innerit Time window S Last nour	
Format Anonymizers and Proxies							Maximum Results 10000	
Application Protocols Search Application Distances Trans	forring Mahupup							
Application Protocols Used	by File Transfers							
Fields Applications Introducing Ma	alware							
Applications by Total Bandy Client Applications	width							Preview
Users Comprehensive Application	List							+ i
File Actions File Categories								
Table File Dispositions							Section Description \$ <time window="">\$<constraints></constraints></time>	
File Names Protect File Transfers over Time							Time Window 🦳 Joherit Time Window 🔿 Last hour	
File Types								
Format File Types Infected with Ma	lware						Maximum Results 10000	
Search Hosts Receiving Files								
the standard standards and standards								
Hosts Receiving Malware								
Fields Hosts Sending Files		•						

Add a Preset Value

Step 7. Select the ${\rm Table} \; {\rm View} \;$ as the output format as shown in the image.

CISCO Overview / Reporting / Report Template Designer Overview	Analysis Po	licies Devices	Objects	AMP	Intelligence	Deploy (λ 🚱	0	adr	ain
Reports Report Templates										
Report Title +						Generate	Adva	inced	Sa	ve
Report Sections							l E C	п в	т	i i
Table View of Events									+	Û
Table User Activity ▼ Preset None ▼ Format ■ □ Search None ▼ Fields Time Event Username Realm Dic ✓]				Section Description \$ <time window="">\$<constraints> Time Window inherit Time Window • Last hour Maximum Results 10000</constraints></time>					
									Preview	e
🖬 🔻 Users									+	Ì
Table User Activity Preset None					Section Description S <time window="">S<constraints></constraints></time>					
Format L C L	/				Maximum Results 10000					
									Preview	e

Table View as Output Format

Step 8. (Optional) From the search menu, select the attributes you want to use to constrain the report. Select None if you do not want to enforce any search constraints.

Search Information	
Table User Activity	
Saved Searches	
None 💌	
Search Information	
Event	New User, Login, Delete, Dropped
Username	jsmith
Realm	REALM
Discovery Application	Idap
Authentication Type	No Authentication, Active Authentication
IP Address	+ 192.168.1.0/24, 1192.168.1.3, 2001.db8.85a3::1370
Start Port	2300
End Port	2500
Description	jdoe
VPN Session Type	AnyConnect IKEv2, AnyConnect SSL, *IKEv2
VPN Group Policy	MyGroupPolicy

Search Constraints

Step 9. Select the time frame for which you want to generate the report. Click on Last hour and a new pop-up window will open with options of 1 hour, 6 hours, 1 day, 1 month, and so on as shown in the image.

Cisco Firepower Ma	anagement Center ng / Report Template Designer	Overview	Analysis	Policies	Devices	Objects	AMP	Intelligence	Deploy Q 🗳 🌣 🔞 admi
Reports Report Temp	plates								
Report Title VPN User Activity Report	+								Generate Advanced Save
Report Sections									
Table View of Event	S								+ ī
Table Preset Format Search Fields	User Activity None M ピ ♥ III None Time, Event, Username, Real	v v Im, Di:	/					Section Description \$ <time window="">\$<constraints> Time Window Last hour Maximum Results 10000</constraints></time>	
m - Hears									Preview
III ♥ Osers									+
Table	User Activity	•						Section Description \$ <time window="">\$<constraints></constraints></time>	
Preset	None	•						Time Window 🔄 Inherit Time Window 🥥 Last hour	
Format	H F C II							Maximum Results 10000	
Search	None	Ŧ	/						
Fields	Count, Username	/							
									Preview

Select Time Frame

Events Time Window Preferences	
Sliding Time Window 🔹	Presets
Show the Last 1 hour(s) 🔻	LastSynchronize with1 hourAudit Log Time Window6 hoursHealth Monitoring Time1 dayWindow1 weeksHealth Health
	Any changes made will take effect on the next page load.

Add TimeFrame

Step 10. To record the specific number of results, provide any value between the range of 1 - 400000 in Maximum Results field.

Report Table Cenerate Advanced Save VPN User Activity Report + Cenerate Advanced Save Report Table Cenerate Advanced Save Report Table Cenerate Advanced Save If v Table Cenerate Advanced Save If v Table Cenerate Cenerate Advanced Save If v Table Cenerate Cenerat Cenerate Cen	Firepower Ma	anagement Center ng / Report Template Designer Overview	v Analysis	Policies	Devices	Objects	AMP	Intelligence	Deploy Q 💕 🌣 🙆 admir
Report Title Generate Advanced Ser VPN User Activity Report + -	Reports Report Temp	olates							
Report Sections In L C C III E T E If v Table View of Events + Table User Activity • Preset None Format Ime View of Events Format Ime View of Events Fields Time, Event, Username, Realm, Dit Im v Users • Table User Activity Im v Users •	Report Title VPN User Activity Report	+							Generate Advanced Save
III ▼ Table View of Events + Table User Activity ▼ Preset None Format IIII Search None Fields Time, Event, Username, Realm, Dit	Report Sections								
Table User Activity Section Description \$ <time window="">\$<constraints> ^ Preset None Time Window Last hour Format Imode Imode Imode Fields Time, Event, Username, Realm, Dit Imode Imode Imode Veset Veset Imode Imode Table User Activity Section Description \$<time window="">\$<constraints> Imode Table User Activity Section Description \$<time window="">\$<constraints> Imode</constraints></time></constraints></time></constraints></time>	Table View of Events	S							+ 1
Preset None Format Imit I I I I I I I I I I I I I I I I I I I	Table	User Activity	•					Section Description \$ <time window="">\$<constraints></constraints></time>	
Format Maximum Results 10000 Search None Image: Comparison of the search	Preset	None	-					Time Window 📋 Inherit Time Window 👩 Last hour	
Search None Image: Constraints Fields Time, Event, Username, Realm, Dit Image: Constraints Image: Constraints Image: Constraints	Format	HK C III	_					Maximum Results 10000	
Fields Time, Event, Username, Realm, Dir Preview III v Users + i Table User Activity Section Description	Search	None	/						
Preview Table User Activity Section Description \$ <time windows\$<constraints=""></time>	Fields	Time, Event, Username, Realm, Di:							
Table User Activity Section Description \$ <time window="">\$<constraints></constraints></time>									Preview
Table User Activity Section Description \$ <time window="">\$<constraints></constraints></time>	🖬 🔻 Users								+ 1
	Table	User Activity	·					Section Description \$ <time window="">\$<constraints></constraints></time>	
Preset None Time Window Data hour	Preset	None	-					Time Window 🗌 Inherit Time Window 🛛 Last hour	
Format Maximum Results 10000	Format	<u>ы</u> ⊻ € <u> </u>						Maximum Results 10000	
Search None V	Search	None	/						
Fields Count, Username	Fields	Count, Username							
Proview									Preview

Maximum Results to display

Step 11. Click on the ${\rm Save}\,$ button at the top of the report sections for the template to be ready for use.

Firepower Management Center Overview / Reporting / Report Template Dec	igner Overview	Analysis	Policies	Devices	Objects	AMP	Intelligence	Deploy C	2 🧬 i	¢ 0	admin •
Reports Report Templates											
Report Title +								Generate	Adva	nced	Save
Report Sections								In	l E C	п в	твы
Table View of Events											+ 🗑
Table User Activity	•						Section Description \$ <time window="">\$<constraints></constraints></time>				
Preset None							Time Window 🗌 Inherit Time Window 🔮 Last hour				
Format 🔟 ピ 🔟							Maximum Results 10000				
Search None	•	/									
Fields Time, Event, Usernan	ne, Realm, Di: 🥒										
										-	review
III V Users											+ 🗑
Table User Activity	•						Section Description \$ <time window="">\$<constraints></constraints></time>				
Preset None	•						Time Window 🗌 Inherit Time Window 🕥 Last hour				
Format 📶 ピ 🗰							Maximum Results 10000				
Search None	٣	/									
Fields Count, Username	/										
										F	review

Save Report

Generate Report

Once you create and customize your report template, you are ready to generate the report. There are different output formats like HTML, PDF or CSV to view the user data.



Note: For PDF reports, file names using Unicode (UTF-8) characters are not supported.

Procedure

Step 1. Select Overview > Reporting and click on Report Templates.

Step 2. Click on the Generate Report icon next to the template that you have configured as shown in the image.

CISCO Overview / Reporting / Report Templates	Overview	Analysis	Policies	Devices	Objects	AMP	Intelligence	Deploy Q 🥩 🌣 🥥 admin '
Reports Report Templates								
								Create Report Template
Risk Report Templates					Last Modifie	d		
Advanced Malware Risk Report					2023-10-31 Modified by	08:11:02 "admin"		0 % C / 3
Attacks Risk Report					2023-10-3 Modified by	08:11:02 "admin"		
Network Risk Report					2023-10-31 Modified by	08:11:02 "admin"		日本でメー
Templates					Last Modifie	d		
Attack Report: \$ <attack sid=""></attack>					2023-04-05 Modified by	07:28:40 "admin"		8 % C / ¥
Files Report					2023-04-05 Modified by	07:28:41 "admin"		0 % C / ¥
FirePOWER Report: \$ <customer name=""></customer>					2023-04-05 Modified by	07:28:41 "admin"		
Host Report: \$ <host></host>					2023-04-05 Modified by	07:28:41 "admin"		0 % C / ¥
Malware Report					2023-04-05 Modified by	07:28:41 "admin"		
Report of User Activity					2023-10-12 Modified by	03:17:13 "admin"		8 % C / 8
Report of VPN Troubleshooting					2023-10-12 Modified by	02:29:58 "admin"		0 % C / ¥
TZ-VPN-Report					2023-10-12 Modified by	05:22:24 "admin"		
User Report: \$ <user></user>					2023-04-05 Modified by	07:28:41 "admin"		8 % C / \$
VPN User Activity Report					2023-10-31 Modified by	08:05:17 "admin"		□ № ℃ / ¥
new-test-vpn					2023-10-31 Modified by	07:37:46 "admin"		8 % C / 8

Generate Reports View

Step 3. Enter a new File Name. This name is used to save the report. If you do not enter a new name, the system uses the default name specified in the report template.

Generate Report

Report Generation Information



Add Filename

Step 4. Choose the output format for the report by clicking: HTML, PDF, or CSV.



Select File Output Format

Step 5. (Optional) Change the global time frame for the report from "Time Window". This gets ignored if "Inherit Time Window" is not used in the report template.



Note: Setting the global time window affects the content of individual report sections only if they are configured to inherit the global setting.

Step 6. (Optional) If the generated report has to be delivered via email, configure a "Relay Host" on the FMC.

Step 7. Click on Generate and files will be available for download under "Reports". For CSV format, a zip folder will be created with each section of the template as a separate file.



Report Generated

Result

This section provides the information of the report generated for the VPN user in a PDF format.

Table View of Users	
---------------------	--

Time Window: 2023-10-01 11:21:25 - 2023-10-01 13:02:03

User	Last Seen	Realm	Username	First Name	Last Name	E-Mail	Department	Phone	Discovery Application	Active Session Count	Available For Policy
cisco-Idapicisco-Idap (LDAP)	2023-10-01 13:00:56	cisco-ldap	cisco-Idap						LDAP	1	no
cisco-local\admin (LDAP)	2023-10-01 10:05:12	cisco-local	admin						LDAP	0	no
Discovered Identities\cisco-radius (LDAP)	2023-10-01 09:45:44	Discovered Identities	cisco-radius						LDAP	0	no
lleare											

Users	
Time Window: 2	023-10-01 11:21:25 - 2023-10-01 13:02:03
Count	

Count	User
1	cisco-ldap/cisco-ldap (LDAP)
1	cisco-local/admin (LDAP)
1	Discovered Identities/cisco-rar

Discovered Identities/cisco-radius (LDAP)

View Generated Reports