# 为VPN用户生成FMC报告

### 目录

<u>简介</u>			
<u>先决条件</u>			
<u>要求</u>			
使用的组件			
<u>背景信息</u>			
<u>配置</u>			
<u>配置</u>			
<u>生成报告</u>			
<u>步骤</u>			
<u>结果</u>			

### 简介

本文档介绍如何生成报告,提供有关VPN用户的整合信息的概览视图,包括用户的当前状态、设备 类型、客户端操作系统、客户端应用和Firepower管理中心上的连接持续时间。

### 先决条件

### 要求

Cisco建议您了解以下主题:

- 思科Firepower威胁防御(FTD)
- 思科Firepower管理中心(FMC)
- AnyConnect 安全移动客户端

#### 使用的组件

本文档中的信息基于以下软件版本:

- 适用于VMware的Cisco FMC(7.x版)
- AnyConnect安全移动客户端4.x

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原 始(默认)配置。如果您的网络处于活动状态,请确保您了解所有命令的潜在影响。

### 背景信息

Firepower系统提供灵活的报告系统,使您可以快速轻松地生成有关Firepower管理中心的报告。您

还可以从头设计自定义报告。报告是以PDF、HTML或CSV格式设置的文档文件,包含您要通信的 内容,而报告模板指定报告及其部分的数据搜索和格式。Firepower系统包括一个功能强大的报告设 计器,可自动设计报告模板。您可以在模板中包含身份验证类型、连接持续时间等字段参数,以扩 展其实用性。

远程访问VPN为远程用户(如移动用户或远程工作者)提供安全连接。监控这些连接可快速提供连 接和用户会话性能的重要指标。您必须是枝叶域中的管理员用户才能执行此任务。 通过 Firepower系统监控功能,您可以快速确定是否存在远程访问VPN问题,然后应用此知识并使用网络 管理工具减少或消除网络和用户的问题。

### 配置

#### 配置

步骤1:选择Overview > Dashboards > Reporting > Report Templates,然后单击Create Report Template,如图所示。

Firepower Management Center Overview / Reporting / Report Templates	Overview Analysis Policier	s Devices Objects	AMP Intelligence	Deploy 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	reporting	Discovery Performance	1:05:21 Imin"	■ % ≥ × %
Attacks Risk Report		Connection Summary	1:05:21 Imin*	■版化/育
Network Risk Report		2023-10-31 Modified by	1.08:05:21 "admin"	■ % C × %
Templates		Last Modifier	rd	
Attack Report: \$ <attack sid=""></attack>		2023-04-05 Modified by	5 07:28:40 "admin"	0 % C / ¥
Files Report		2023-04-05 Modified by	5 07:28:41 "admin"	日本 ビノネ
FirePOWER Report: \$ <customer name=""></customer>		2023-04-05 Modified by	5 07:28:41 "admin"	8 % C / 9
Host Report: \$ <host></host>		2023-04-05 Modified by	5 07:28:41 "admin"	0 % C / 9
Malware Report		2023-04-05 Modified by	5 07:28:41 "admin"	日本 ビノネ
Report of User Activity		2023-10-17 Modified by	7 03:17:13 "admin"	8 % C / ¥
Report of VPN Troubleshooting		2023-10-12 Modified by	2 02:29:58 "admin"	日本 ピノネ
TZ-VPN-Report		2023-10-17 Modified by	7 05:22:24 "admin"	8 % C / 9
User Report: \$ <user></user>		2023-04-05 Modified by	5 07:28:41 "admin"	0 % C / 9
VPN User Activity Report		2023-10-31 Modified by	1 08:05:17 "admin"	8 % C / V
new-test-vpn		2023-10-31 Modified by	1 07:37:46 "admin"	8 % C / ¥

创建报告模板

#### 第二步:在Report Title字段中输入模板的名称,如图所示。

Firepower Management Center Overview / Reporting / Report Template Designer	Overview	Analysis	Policies	Devices	Objects	AMP	Intelligence	Dep	by Q	¢	¢	0	admin 🔻
Reports Report Templates													
Report Title								Gene	rate	Ad	vanceo	1	Save
Report Sections									ы	⊻ €	; III	• 1	89
				No Secti	ons								

报告标题

第三步:从右侧的一组可用视图中选择Add Table View。您还可以根据需要使用条形图、折线图、饼图等图表。

Firepower Management Center Overview / Reporting / Report Template Designer	Overview	Analysis	Policies	Devices	Objects	AMP	Intelligence	 Deploy	۹	¢	₽	0	admin 🔻
Reports Report Templates													
Report Title VPN User Activity Report +								Generat	c	Adv	anced		Save
Report Sections									ыĿ	~ C	Π	ВT	E 59
				No Secti	ions								

添加表视图

#### 第四步:在Report Section Title字段中输入部分的标题。此处添加了Table View of Events和Users表视图,如图所示。

Gisco Overview / Report	anagement Center ing / Report Template Designer	Overview	Analysis	Policies	Devices	Objects	AMP	Intelligence			Deploy Q 🧬	¢ (	adı	min •
Reports Report Tem	plates													
Report Title VPN User Activity Report	+										Generate Adv	anced	S	ave
Report Sections											브 년 6	II B	т	5
Table View of Event	ts												+	Ì
Table	User Activity	Ŧ						Section Description	\$ <time window="">\$<constraints></constraints></time>	/				
Prese	None	•						Time Window	v 🗌 Inherit Time Window 🛛 🕲 Last	hour				
Forma	<b>Ⅲ № € </b> Ⅲ							Maximum Results	s 10000					
Search	None	•	/											
Fields	Time, Event, Username, Real	m, Di: !												
													Preview	w
₩ Users													+	¥
Table	User Activity	•						Section Description	\$ <time window="">\$<constraints></constraints></time>	/				
Prese	None	*						Time Window	v 🗌 Inherit Time Window 🔮 Last	hour				
Formal	<b>ы</b> К <b>с</b> III							Maximum Results	s 10000					
Search	None	Ψ.	/											
Fields	Count, Username	/												
													Preview	w

报告部分的标题

#### 第五步:在Table下拉菜单中选择User Activity(如图所示)。

Cisco Overview / Reporting / Report Template Designer Overview	Analysis	Policies	Devices	Objects	AMP	Intelligence	Deploy Q 💣 🌣 🛛 admir	in •
Reports Report Templates								
Report Title +							Generate Advanced Save	e
Report Sections							<b>MKCHETE</b>	5
Table View of Events							+ ÿ	i.
Table User Activity  Preset Intrusion Events with Destination Criticality Intrusion Events with Source Criticality Format QoS Ruls Statistics Search Rule Update Import Log Situation Fields Scan Results Scan Result	-					Section Description \$ <time window="">\$<constraints> Time Window   Inherit Time Window @ Last hour Maximum Results 10000</constraints></time>		
Security Intelligence Statistics	-						Preview	2
Third: Party Vulnerabilities URL Category Statistics URL Reputation Statistics URL Reputation Statistics URL Reputation Statistics User Statistics Format User Statistics Format Vers Trobueshooting Search Vulnerabilities	-					Section Description S <time window="">S<constraints> Time Window Inherit Time Window O Last hour Maximum Results 10000</constraints></time>		
ricus Courk, Usemaine P							Preview	

选择用户活动

### 第六步:如果需要,请选择一个预设值,否则,请保留其为None。

cisco Overview /	Ver Management Center / Reporting / Report Template Designer	Overview	Analysis	Policies	Devices	Objects	AMP	Intelligence	Deploy Q 🗳 🌣 🛿 admir
Reports Repo	ort Templates								
Report Title									Generate Advanced Save
VPN User Activity	Report +								
Report Sections	\$								<b>MEGHETE</b>
III 🔻 Table View of	of Events								+ ī
	Table User Activity	-						Section Description \$ <time window="">\$<constraints></constraints></time>	
	Dragat Nees	_						Time Window 🖂 Jaharit Time Window 🔿 Last hour	
	None None	¥	193					Time window	
	Format Anonymizers and Proxies							Maximum Results 10000	
	Application Protocols Search Application Distancels Transfe	arrian Mahunan							
	Application Protocols transfe Application Protocols Used b	by File Transfers							
	Fields Applications Introducing Mal	ware							
	Client Applications	idth							Preview
🖬 🔻 Users	Comprehensive Application I	List							+ ī
	File Actions File Categories								
	Table File Dispositions							Section Description \$ <time window="">\$<constraints></constraints></time>	
	File Names							Time Window 🖂 Joharit Time Window 🔿 Last hour	
	File Types								
	Format File Types Infected with Mah	ware						Maximum Results 10000	
	Granular Application Usage Search Hosts Receiving Files								
	Hosts Receiving Malware								
	Fields Hosts Sending Files		*						

添加预设值

#### 步骤 7.选择Table View作为输出格式,如图所示。

Cisco Overview / Reporting	nagement Center 7 / Report Template Designer	Overview	Analysis	Policies	Devices	Objects	AMP	Intelligence	Deploy Q 🗳 🌣 🔞 admir
Reports Report Templa	ates								
Report Title VPN User Activity Report	+								Generate Advanced Save
Report Sections									
Table View of Events									+ 1
Table [ Preset ] Format [ Search ]	User Activity None None	* *	,					Section Description \$ <time window="">\$<constraints> Time Window    Inherit Time Window    Last hour Maximum Results 10000</constraints></time>	
Fields	Time, Event, Username, Realing	m, Die							Preview
🖬 🔻 Users									+ ĩ
Table	User Activity	٣						Section Description \$ <time window="">\$<constraints></constraints></time>	
Preset	None	Ψ.						Time Window 🗌 Inherit Time Window 🛛 Last hour	
Format [	<u>ы к с ш</u>							Maximum Results 10000	
Search	None	Ψ.	/						
Fields	Count, Username	/							Province

作为输出格式的表格视图

第8步(可选)从搜索菜单中,选择要用于限制报告的属性。如果不希望强制实施任何搜索限制,请选择None。

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.db8.85e3.1370
Start Port	2300
End Port	2500
Description	jdoe
VPN Session Type	AnyConnect IKEv2, AnyConnect SSL, *IKEv2
VPN Group Policy	MyGroupPolicy

搜索限制

步骤 9选择要为其生成报表的时间范围。点击Last hour,新的弹出窗口将打开,选项包括1小时、6小时、1天、1个月等,如图所 示。

Gisco Firepower Management C Overview / Reporting / Report Temple	enter te Designer	Analysis	Policies	Devices	Objects	AMP	Intelligence	Deploy Q 🔮	° 0	admin
Reports Report Templates										
Report Title VPN User Activity Report +								Generate Adva	inced	Save
Report Sections								<u> 비</u> 년 6	ш в	TES
Table View of Events										+ 🗑
Table User Activity Preset None Format ML L⊻ @ [1] Search None	* *	,					Section Description S <time window="">S<constraints> Time Window  Last hour Maximum Results 10000</constraints></time>			
Fields Time, Event, U	sername, Realm, Di: 🖌								P	review
🖬 🔻 Users										+ 🗑
Table User Activity Preset None Format Int 200 III Search None	* *   *	/					Section Description \$ <time window="">\$<constraints> Time Window</constraints></time>			
Fields Count, Userna	ne 🖌								P	review

选择时间范围

Events Time Window	Preferences		
Sliding Time Window	•	Presets	
Show the Last 1	nour(s) 🔻	Last 1 hour 6 hours 1 day 1 week 2 weeks 1 month	Synchronize with Audit Log Time Window Health Monitoring Time Window
			Any changes made will take effect on the next page load.
			Reset

添加时间范围

#### 步骤 10要记录特定结果数,请在Maximum Results字段中提供1到400000之间的任何值。

Gisco Firepower Ma	nagement Center g / Report Template Designer	Overview	Analysis	Policies	Devices	Objects	AMP	Intelligence	Deploy Q	¢ 🗘	🛛 admi
Reports Report Templ	lates										
Report Title VPN User Activity Report	+								Generate	Advanced	Save
Report Sections									<u>ы</u> (2	C III	B T E
Table View of Events											+ i
Table	User Activity	Ψ.						Section Description \$ <time window="">\$<constraints></constraints></time>			
Preset	None	•						Time Window 📋 Inherit Time Window 🥥 Last hour			
Format	<u>ы к с Ш</u>							Maximum Results 10000			
Search	None	•	/								
Fields	Time, Event, Username, Realm	n, Di: 🖉									
											Preview
🖬 🔻 Users											+ i
Table	User Activity	٣						Section Description \$ <time window="">\$<constraints></constraints></time>			
Preset	None	Ŧ						Time Window 🔄 Inherit Time Window 🕥 Last hour			
Format	<u>ы</u> К С Ш							Maximum Results 10000			
Search	None	•	/								
Fields	Count, Username	/									
											Preview

要显示的最大结果

步骤 11点击报告部分顶部的Save按钮,模板即可使用。

Firepower Manag Overview / Reporting / Re	ement Center eport Template Designer	Verview	Analysis	Policies	Devices	Objects	AMP	Intelligence	Deploy C	¢ 💞	¢ 6	admin •
Reports Report Templates												
Report Title VPN User Activity Report	+								Generate	Adv	inced	Save
Report Sections									ы	1 E C	ш в	TES
Table View of Events												+ 🗑
Table Use	er Activity	Ŧ						Section Description \$ <time window="">\$<constraints></constraints></time>				
Preset Nor	ne							Time Window 🗌 Inherit Time Window 🔮 Last hour				
Format M	K C III							Maximum Results 10000				
Search Nor	ne	٣	/									
Fields Tim	ne, Event, Username, Realm, D	Die 🖉										
												Preview
III ▼ Users												+ 🗑
Table Use	er Activity	*						Section Description \$ <time window="">\$<constraints></constraints></time>				
Preset Nor	ne							Time Window 🗌 Inherit Time Window 🕥 Last hour				
Format 🔟	E C III							Maximum Results 10000				
Search Nor	ne	۳	/									
Fields Con	unt, Username	/										
												Preview

保存报告

生成报告

创建并自定义报告模板后,即可生成报告。有多种不同的输出格式,如HTML、PDF或CSV,可用来查看用户数据。



注意:对于PDF报告,不支持使用Unicode (UTF-8)字符的文件名。

步骤

步骤1:选择Overview > Reporting ,然后单击Report Templates。

第二步:点击已配置模板旁边的Generate Report图标,如图所示。

Firepower Management Center Overview / Reporting / Report Templates	Overview Analysis	Policies Devi	oes Objects	AMP I	ntelligence	Deploy Q 🗳 🌣 🥥 admin '
Reports Report Templates						
						Create Report Template
Risk Report Templates			Last Modified			
Advanced Malware Risk Report			2023-10-31 Modified by "	08:11:02 admin"		日日ビノ市
Attacks Risk Report			2023-10-31 Modified by *	08:11:02 admin*		日日にノ市
Network Risk Report			2023-10-31 Modified by "	08:11:02 admin*		日本ビノ主
Templates			Last Modified			
Attack Report: \$ <attack sid=""></attack>			2023-04-05 Modified by "	07:28:40 admin*		6 % C / V
Files Report			2023-04-05 Modified by "	07:28:41 admin"		8 % C / V
FirePOWER Report: \$ <customer name=""></customer>			2023-04-05 Modified by "	07:28:41 admin*		8 % C / V
Host Report: \$ <host></host>			2023-04-05 Modified by "	07:28:41 admin*		日 9 년 / 第
Malware Report			2023-04-05 Modified by "	07:28:41 admin*		■ % C / ¥
Report of User Activity			2023-10-17 Modified by	03:17:13 admin*		8 % C / P
Report of VPN Troubleshooting			2023-10-12 Modified by "	02:29:58 admin*		■ <b>● ● /</b> ●
TZ-VPN-Report			2023-10-17 Modified by *	05:22:24 admin*		日本 日子 日
User Report: \$ <user></user>			2023-04-05 Modified by "	07:28:41 admin"		日本 化 / 第
VPN User Activity Report			2023-10-31 Modified by *	08:05:17 admin*		<b>□</b> 14 C / 14
new-test-vpn			2023-10-31 Modified by *	07:37:46 admin*		8 % C / ¥

生成报告视图

第三步:输入新的文件名。此名称用于保存报告。如果不输入新名称,系统将使用报告模板中指定的默认名称。

## Generate Report

### **Report Generation Information**



添加文件名

第四步:通过点击选择报告的输出格式:HTML、PDF或CSV。



选择文件输出格式

第5步(可选)从"时间窗口"更改报告的全局时间范围。如果报告模板中未使用"Inherit Time Window",则会忽略此项。



注:只有当单个报告部分配置为继承全局设置时,设置全局时间窗口才会影响其内容。

第6步:(可选)如果生成的报告必须通过邮件发送,请在FMC上<u>配置</u>"中继主机"。

步骤 7.点击Generate,文件将在"Reports"下可供下载。对于CSV格式,将创建一个zip文件夹,将模板的每个部分作为单独的文件。



2023-11-06 22:09:26

2023-11-06 22:09:27

Local

admin

Successfully Processed

报表生成于

#### 结果

本节以PDF格式提供为VPN用户生成的报告的信息。

Table View of Users	1
---------------------	---

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-Idap\cisco	ldap (LDAP)	2023-10-01 13:00:56 cisco-ldap		cisco-Idap						LDAP	1	no
cisco-loca/ladmi	ocal/admin (LDAP) 2023-10-01 10:05:12 cisco-loc		cisco-local	admin						LDAP	0	no
Discovered Iden	tities\cisco-radius (LDAP)	2023-10-01 09:45:44	Discovered Identities	cisco-radius						LDAP	0	no
Users Time Window: 2023	-10-01 11:21:25 - 2023-10-01 13	02:03										
Count		User	1									
		store inter	and the second									

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

Discovered Identities/cisco-radius (LDAP)

查看生成的报告

#### 关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言,希望全球的用户都能通过各 自的语言得到支持性的内容。

请注意:即使是最好的机器翻译,其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任,并建议您总是参考英文原始文档(已提供 链接)。