ASA 版本 9.2 VPN SGT 分类和实施配置示例

目录

简介

本文档介绍如何为VPN用户使用自适应安全设备(ASA)版本9.2.1 TrustSec安全组标记(SGT)分类中 的新功能。本示例展示两个VPN用户,它们被分配了不同的SGT和安全组防火墙(SGFW),过滤 VPN用户之间的流量。

先决条件

要求

Cisco 建议您了解以下主题:

- ASA CLI配置和安全套接字层(SSL)VPN配置的基本知识
- ASA上远程访问VPN配置的基本知识
- •身份服务引擎(ISE)和TrustSec服务的基本知识

使用的组件

本文档中的信息基于以下软件版本:

- Cisco ASA软件9.2版及更高版本
- Windows 7与Cisco AnyConnect安全移动客户端,版本3.1
- 思科ISE版本1.2及更高版本

配置

注意:要获取有关本部分中所使用命令的更多信息,可使用命令查找工具(仅限已注册客户)。

网络图

VPN用户"cisco"被分配给财务团队,财务团队可以启动与营销团队的Internet控制消息协议(ICMP)连接。 VPN用户"cisco2"被分配给营销团队,该团队不允许发起任何连接。



ISE 配置

:

- 1. 选择**Administration > Identity Management > Identities**以添加并配置用户"cisco"(来自 Finance)和"cisco2"(来自Marketing)。
- 2. 选择Administration > Network Resources > Network Devices以将ASA添加并配置为网络设备。
- 选择Policy > Results > Authorization > Authorization Profiles以添加和配置财务和营销授权配置文件。两个配置文件仅包含一个允许所有流量的属性,可下载访问控制列表(DACL)。下面是财务示例

cisco Identity Services Engine	
🛓 Authentication 🛛 🧕 Authorization	🔀 Profiling 💿 Posture 🔊 Client Provisioning 📄 Security Group Access
Dictionaries Conditions Results	
Results	Authorization Profiles > Finance_Profile Authorization Profile * Name Finance_Profile Description * Access Type ACCESS_ACCEPT
Client Provisioning	▼ Common Tasks
 Security Group Access 	DACL Name PERMIT_ALL_TRAFFIC -

每个配置文件可以具有特定的限制性DACL,但是对于此情况,允许所有流量。实施由 SGFW执行,而不是分配给每个VPN会话的DACL。使用SGFW过滤的流量仅允许使用 SGT,而不允许DACL使用的IP地址。

4. 选择**Policy > Results > Security Group Access > Security Groups**以添加和配置财务和营销 SGT组。

alada				
cisco Identity Services Engine		🏠 Home O	perations 🔻	Policy 🔻
ዿ Authentication 👩 Authorization	💦 Prot	filing 💽 Posture	💫 Client	t Provisioning
Dictionaries Conditions Results				
Results		Security Group	S	
	5	🧨 Edit 🕂 Add	💽 Import	🕞 Export 🚽
	***	Name 🔺	SGT (Dec /	Hex)
Automication		Finance	2/0002	
Authorization Profiles		Marketing	3/0003	
Downloadable ACLs		Unknown	0/0000	
Inline Posture Node Profiles				
Profiling				
Posture				
 Client Provisioning 				
🔻 🚞 Security Group Access				
Security Group ACLs				
 Security Groups Security Group Mappings 				

5. 选择**Policy > Authorization**以配置两个授权规则。第一条 规则将Finance_profile(允许整个流 量的DACL)以及SGT组Finance分配给"cisco"用户。 第二条 规则将Marketing_profile(允许 整个流量的DACL)以及SGT组Marketing分配给"cisco2"用户。

- alto	die als	ally Condens Friday						
cis	co Idei	nuty Services Engine	🏠 Home	Operations 🔻	Policy 🔻	Administration •		
4	Authentic	ation 🧕 Authorization 🛃	Profiling 🛛 💽 Pos	ture 👩 Client	Provisioning	🚊 Security Group Acce	ss 👌	Policy Elements
Auth	orizati	on Policy						
Define	e the Autho	rization Policy by configuring rules ba	sed on identity groups	and/or other condit	ions. Drag and	drop rules to change the ord	ler.	
First	: Matched	l Rule Applies 🚽						
▶ Ex	ceptions ((0)						
Sta	andard							
	Status	Rule Name	Condition	s (identity groups ar	nd other condit	ions)		Permissions
	2	cisco	if Radius:Us	er-Name EQUALS	cisco		then	Finance_Profile AND Finance
1	~	cisco2	if Radius:Us	er-Name EQUALS	cisco2		then	Marketing_Profile AND Marketing

ASA 配置

1. 完成基本VPN配置。

```
webvpn
enable outside
anyconnect-essentials
anyconnect image disk0:/anyconnect-win-3.1.02040-k9.pkg 1
anyconnect enable
tunnel-group-list enable
```

group-policy GP-SSL internal
group-policy GP-SSL attributes
vpn-tunnel-protocol ikev1 ikev2 ssl-client ssl-clientless

```
tunnel-group RA type remote-access
tunnel-group RA general-attributes
address-pool POOL
authentication-server-group ISE
accounting-server-group ISE
default-group-policy GP-SSL
tunnel-group RA webvpn-attributes
```

ip local pool POOL 10.10.10.10-10.10.10.100 mask 255.255.255.0

2. 完成ASA AAA和TrustSec配置。

group-alias RA enable

```
aaa-server ISE protocol radius
aaa-server ISE (outside) host 10.48.66.74
key *****
cts server-group ISE
为了加入TrustSec云,ASA需要使用保护访问凭证(PAC)进行身份验证。ASA不支持自动
```

PAC调配,因此该文件需要在ISE上手动生成并导入到ASA。

3. 选择Administration > Network Resources > Network Devices > ASA > Advanced TrustSec Settings以便在ISE上生成PAC。选择Out of Band(OOB)PAC调配以生成文件。

cisco Identity Services Engine	Home Operations + Policy + Administration +	
System Methods Network Device Groups Ext	Robert Resources 💽 With Podal Management 📷 Food Service Innal RADIUS Servers RADIUS Server Sequences SGA AAA Servers NAC Managers MDM	
Network Devices	* Reauthentication every 1 0995 * Download 60ACL lists every 1 0995 * Download 60ACL lists every 1 0995 * Download 60ACL lists every 1 0995 * Other 504 deverant in functions dever 0 The former at the active active * The identity find device about * * * The identity find device about * * * The identity find device * * * * The identity find device *	× col.
	▼ Out Of Band (DOB) SGA PAC	
	Issue Date 16 Mar 2014 16:40:25 C	
	Insued By admin Generate FAC	

4. 将PAC导入ASA。生成的文件可以放在HTTP/FTP服务器上。ASA使用它导入文件。

ASA# cts import-pac http://192.168.111.1/ASA-CTS-2.pac password 12345678

```
!PAC Imported Successfully
ASA#
ASA# show cts pac
PAC-Info:
  Valid until: Mar 16 2015 17:40:25
  ATD:
              ea48096688d96ef7b94c679a17bdad6f
              ASA-CTS-2
  I-ID:
  A-ID-Info: Identity Services Engine
  PAC-type:
              Cisco Trustsec
PAC-Opaque:
  000200b80003000100040010ea48096688d96ef7b94c679a17bdad6f0006009c000301
  0015e3473e728ae73cc905887bdc8d3cee00000013532150cc00093a8064f7ec374555
  e7b1fd5abccb17de31b9049066f1a791e87275b9dd10602a9cb4f841f2a7d98486b2cb
  2b5dc3449f67c17f64d12d481be6627e4076a2a63d642323b759234ab747735a03e01b
  99be241bb1f38a9a47a466ea64ea334bf51917bd9aa9ee3cf8d401dc39135919396223
  11d8378829cc007b91ced9117a
当您拥有正确的PAC时,ASA会自动执行环境刷新。这会从ISE下载有关当前SGT组的信息。
ASA# show cts environment-data sg-table
```

Security Group Table: Valid until: 17:48:12 CET Mar 17 2014 Showing 4 of 4 entries

Marketing	3	unicast
Finance	2	unicast
Unknown	0	unicast
ANY	65535	unicast
SG Name	SG Tag	Туре

5. 配置SGFW。最后一步是在外部接口上配置ACL,允许从财务到营销的ICMP流量。

access-list outside extended permit icmp security-group tag 2 any security-group

tag 3 any

access-group outside in interface outside

此外,可以使用安全组名称代替标记。

access-list outside extended permit icmp **security-group name Finance** any

security-group name Marketing any

为了确保接口ACL处理VPN流量,必须禁用默认情况下允许未经接口ACL验证的VPN流量的选 项。

no sysopt connection permit-vpn

现在,ASA应准备好对VPN用户进行分类,并根据SGT执行实施。

验证

使用本部分可确认配置能否正常运行。

此 <u>输出解释程序工具</u> (<u>已注册</u> 仅客户)支持 show 命令。使用输出解释程序工具查看分析 show 命令 输出.

建立VPN后,ASA显示应用于每个会话的SGT。

ASA(config)# show vpn-sessiondb anyconnect

Session Type: AnyConnect

:	cisco	Index	: 1
:	10.10.10.10	Public IP	: 192.168.10.68
:	AnyConnect-Parent SSL-	Tunnel DTLS-T	'unnel
:	AnyConnect Essentials		
:	AnyConnect-Parent: (1)	none SSL-Tun	nel: (1)RC4 DTLS-Tunnel: (1)AES128
:	AnyConnect-Parent: (1)	none SSL-Tun	nel: (1)SHA1 DTLS-Tunnel: (1)SHA1
:	35934	Bytes Rx	: 79714
:	GP-SSL	Tunnel Group	: RA
:	17:49:15 CET Sun Mar 1	6 2014	
:	0h:22m:57s		
:	0h:00m:00s		
:	N/A	VLAN	: none
:	c0a8700a000010005325d6	0b	
:	2:Finance		
:	cisco2	Index	: 2
:	10.10.11	Public IP	: 192.168.10.80
:	AnyConnect-Parent SSL-	Tunnel DTLS-T	unnel
:	AnyConnect Essentials		
:	AnyConnect-Parent: (1):	none SSL-Tun	nel: (1)RC4 DTLS-Tunnel: (1)AES128
:	AnyConnect-Parent: (1):	none SSL-Tun	nel: (1)SHA1 DTLS-Tunnel: (1)SHA1
:	86171	Bytes Rx	: 122480
:	GP-SSL	Tunnel Group	: RA
:	17:52:27 CET Sun Mar 1	6 2014	
:	0h:19m:45s		
:	0h:00m:00s		
:	N/A	VLAN	: none
:	c0a8700a000020005325d6	cb	
:	3:Marketing		
λī	b务(SGT=2)到营销(SG	T=3)的ICMP》	态量。这就是用户"cisco"可以ping用户"cisco2"的
~~~			
	••••••••••••••••••••••••••••••••••••••	<pre>: cisco : 10.10.10.10 : AnyConnect-Parent SSL- : AnyConnect-Parent: (1) : AnyConnect-Parent: (1) : 35934 : GP-SSL : 17:49:15 CET Sun Mar 1 : 0h:22m:57s : 0h:00m:00s : N/A : c0a8700a000010005325d6 : 2:Finance : cisco2 : 10.10.10.11 : AnyConnect-Parent SSL- : AnyConnect-Parent: (1) : AnyConnect-Parent: (1) : AnyConnect-Parent: (1) : 86171 : GP-SSL : 17:52:27 CET Sun Mar 1 : 0h:19m:45s : 0h:00m:00s : N/A : c0a8700a000020005325d6 : 3:Marketing / 财务(SGT=2)到营销(SG</pre>	<pre>: cisco Index : 10.10.10.10 Public IP : AnyConnect-Parent SSL-Tunnel DTLS-T : AnyConnect-Parent: (1)none SSL-Tun : AnyConnect-Parent: (1)none SSL-Tun : 35934 Bytes Rx : GP-SSL Tunnel Group : 17:49:15 CET Sun Mar 16 2014 : 0h:22m:57s : 0h:00m:00s : N/A VLAN : c0a8700a00010005325d60b : 2:Finance : cisco2 Index : 10.10.10.11 Public IP : AnyConnect-Parent SSL-Tunnel DTLS-T : AnyConnect Essentials : AnyConnect-Parent: (1)none SSL-Tun : 86171 Bytes Rx : GP-SSL Tunnel Group : 17:52:27 CET Sun Mar 16 2014 : 0h:19m:45s : 0h:00m:00s : N/A VLAN : c0a8700a00020005325d6cb : 3:Marketing // M\$\$(SGT=2)到营销(SGT=3)的ICMP\$} </pre>

```
C:\Users\admin>ping 10.10.10.11 -S 10.10.10.10

Pinging 10.10.10.11 from 10.10.10.10 with 32 bytes of data:

Reply from 10.10.10.11: bytes=32 time=3ms TTL=128

Reply from 10.10.10.11: bytes=32 time=4ms TTL=128

Reply from 10.10.10.11: bytes=32 time=6ms TTL=128

Reply from 10.10.10.11: bytes=32 time=5ms TTL=128

Ping statistics for 10.10.10.11:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 3ms, Maximum = 6ms, Average = 4ms
```

计数器增加:

ASA(config)# show access-list outside access-list outside; 1 elements; name hash: 0x1a47dec4 access-list outside line 1 extended permit icmp security-group tag 2(name="Finance") any security-group tag 3(name="Marketing") any (hitcnt=4) 0x071f07fc 已创建连接:

Mar 16 2014 18:24:26: %ASA-6-302020: Built inbound ICMP connection for faddr 10.10.10.10/1(LOCAL\cisco, 2:Finance) gaddr 10.10.10.11/0 laddr 10.10.10.11/0(LOCAL\cisco2, 3:Marketing) (cisco) 因为启用了ICMP检测,所以将自动接受返回流量。

当您尝试从营销(SGT=3)ping财务(SGT=2)时:

#### C:\Users\admin>ping 10.10.10.10 -S 10.10.10.11

```
Pinging 10.10.10.10 from 10.10.10.11 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 10.10.10.10:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

#### ASA报告:

Mar 16 2014 18:06:36: %ASA-4-106023: Deny icmp src outside:10.10.10.11(LOCAL\cisco2, 3:Marketing) dst outside:10.10.10(LOCAL\cisco, 2:Finance) (type 8, code 0) by access-group "outside" [0x0, 0x0]

### 故障排除

本部分提供的信息可用于对配置进行故障排除。

请参阅以下文档:

• Catalyst 3750X系列交换机上具有802.1x MACsec的TrustSec云配置示例

• ASA 和 Catalyst 3750X 系列交换机 TrustSec 配置示例和故障排除指南

# 摘要

本文就如何对VPN用户进行分类和执行基本实施给出了一个简单的示例。SGFW还过滤VPN用户与 网络其余部分之间的流量。可以在ASA上使用SXP(TrustSec SGT交换协议)来获取IP和SGT之间 的映射信息。这允许ASA对已正确分类的所有类型的会话(VPN或LAN)执行实施。

在ASA软件版本9.2及更高版本中,ASA还支持RADIUS授权更改(CoA)(RFC 5176)。在成功的 VPN终端安全评估后从ISE发送的RADIUS CoA数据包可以包括cisco-av-pair和SGT,SGT将合规用 户分配到其他(更安全)组。有关更多示例,请参阅"相关信息"部分中的文章。

# 相关信息

- ASA 版本 9.2.1 基于 ISE 的 VPN 安全评估配置示例
- ASA 和 Catalyst 3750X 系列交换机 TrustSec 配置示例和故障排除指南
- <u>Cisco TrustSec交换机配置指南:了解Cisco TrustSec</u>
- 为安全设备用户授权配置外部服务器
- <u>思科 ASA 系列 VPN CLI 配置指南,版本 9.1</u>
- <u>思科身份服务引擎用户指南,版本 1.2</u>
- <u>技术支持和文档 Cisco Systems</u>

#### 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)。