# ASA 9.2版VPN SGT分類和實施配置示例

# 目錄

# 簡介

本文檔介紹如何在VPN使用者的自適應安全裝置(ASA)版本9.2.1 TrustSec安全組標籤(SGT)分類中 使用新功能。此範例顯示兩個VPN使用者,他們被指派了不同的SGT和安全組防火牆(SGFW),該 防火牆過濾VPN使用者之間的流量。

### 必要條件

#### 需求

思科建議您瞭解以下主題:

- ASA CLI配置和安全套接字層(SSL)VPN配置的基本知識
- ASA上遠端訪問VPN配置的基本知識
- •身份服務引擎(ISE)和TrustSec服務的基本知識

### 採用元件

本檔案中的資訊是根據以下軟體版本:

- Cisco ASA軟體9.2版及更高版本
- Windows 7和Cisco AnyConnect安全移動客戶端,版本3.1
- Cisco ISE版本1.2及更高版本

註:使用<u>命令查詢工具(</u>僅限<u>註冊</u>客戶)可獲取本節中使用的命令的詳細資訊。

### 網路圖表

VPN使用者「cisco」被分配給財務團隊,財務團隊可以啟動與市場行銷團隊的網際網路控制消息協定(ICMP)連線。 VPN使用者「cisco2」被分配給市場行銷團隊,該團隊不允許發起任何連線。



### ISE 組態

:

- 1. 選擇Administration > Identity Management > Identities,以新增並配置使用者「cisco」(來自 Finance)和「cisco2」(來自Marketing)。
- 2. 選擇Administration > Network Resources > Network Devices,以便將ASA新增並配置為網路 裝置。
- 選擇Policy > Results > Authorization > Authorization Profiles以新增並配置Finance and Marketing授權配置檔案。兩個設定檔僅包括一個允許所有流量的屬性,可下載存取控制清單 (DACL)。下面顯示了Finance的一個示例

cisco Identity Services Engine	Administration   ▼
🛃 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  Service Template
<ul> <li>Security Group Access</li> </ul>	DACL Name PERMIT_ALL_TRAFFIC -

每個配置檔案可以具有特定的限制性DACL,但是對於此情況,允許所有流量。實施由 SGFW執行,而不是分配給每個VPN會話的DACL。使用SGFW過濾的流量僅允許使用 SGT,而非DACL使用的IP地址。

4. 選擇**Policy > Results > Security Group Access > Security Groups**,以新增和配置Finance and Marketing SGT組。

alada				
cisco Identity Services Engine		🏠 Home O	perations   🔻	Policy   🔻
🚨 Authentication 🛛 🧕 Authorization	🔏 Profilin	g 💽 Posture	🔊 Client	t Provisioning
Dictionaries Conditions Results				
Results	Se	ecurity Group	S	
		🕈 Edit 🕂 Add	🕞 Import	🚯 Export 🚽
	TH ▼	Name 🔺	SGT (Dec /	Hex)
		] Finance	2/0002	
Authorization Profiles		Marketing	3/0003	
Downloadable ACLs		] Unknown	0/0000	
Inline Posture Node Profiles				
Profiling				
Posture				
<ul> <li>Client Provisioning</li> </ul>				
🔻 🚞 Security Group Access				
Security Group ACLs				
<ul> <li>Security Groups</li> <li>Security Group Mappings</li> </ul>	:			

5. 選擇**Policy > Authorization**以配置兩個授權規則。第一條 規則將Finance\_profile(允許整個流 量的DACL)以及SGT組Finance分配給「cisco」使用者。 第二條 規則將 Marketing\_profile(允許整個流量的DACL)以及SGT組Marketing分配給「cisco2」使用者。

- alto	ultulu Identity Comicas Englas							
cisco Identity 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	<b>~</b>	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
group-alias RA enable
```

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。

aaa-server ISE protocol radius aaa-server ISE (outside) host 10.48.66.74 key \*\*\*\*\* cts server-group ISE 為了加入TrustSec雲,ASA需要使用保護訪

為了加入TrustSec雲,ASA需要使用保護訪問憑證(PAC)進行身份驗證。ASA不支援自動 PAC調配,因此該檔案需要在ISE上手動生成並匯入到ASA。

3. 選擇Administration > Network Resources > Network Devices > ASA > Advanced TrustSec Settings以便在ISE上生成PAC。選擇Out of Band(OOB)PAC設定以生成檔案。

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. 將PAC匯入ASA。生成的檔案可以放在HTTP/FTP伺服器上。ASA使用它匯入檔案。

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
              ea48096688d96ef7b94c679a17bdad6f
  ATD:
              ASA-CTS-2
  I-ID:
  A-ID-Info: Identity Services Engine
  PAC-type:
              Cisco Trustsec
PAC-Opaque:
  000200b80003000100040010ea48096688d96ef7b94c679a17bdad6f0006009c000301
  0015e3473e728ae73cc905887bdc8d3cee00000013532150cc00093a8064f7ec374555
  e7b1fd5abccb17de31b9049066f1a791e87275b9dd10602a9cb4f841f2a7d98486b2cb
  2b5dc3449f67c17f64d12d481be6627e4076a2a63d642323b759234ab747735a03e01b
  99be241bb1f38a9a47a466ea64ea334bf51917bd9aa9ee3cf8d401dc39135919396223
  11d8378829cc007b91ced9117a
當您擁有正確的PAC時,ASA會自動執行環境刷新。從ISE下載有關當前SGT組的資訊。
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。最後一步是在允許從金融到行銷的ICMP流量的外部介面上配置ACL。

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

tag 3 any

access-group outside in interface outside

#### 此外,可以使用安全組名稱代替標籤。

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

security-group name Marketing any

為了確保介面ACL處理VPN流量,必須禁用預設情況下允許未經介面ACL驗證的VPN流量的選 項。

no sysopt connection permit-vpn

現在,ASA應準備好對VPN使用者進行分類,並根據SGT執行實施。

# 驗證

使用本節內容,確認您的組態是否正常運作。

其 <u>輸出直譯器工具</u> (<u>已註冊</u> 僅客戶)支援某些 **顯示** 指令。使用輸出直譯器工具檢視分析 **顯示** 命令 輸出。

在建立VPN後,ASA顯示應用於每個會話的SGT。

ASA(config)# show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username	:	cisco	Index	: 1
Assigned IP	:	10.10.10.10	Public IP	: 192.168.10.68
Protocol	:	AnyConnect-Parent SSL-7	Cunnel DTLS-T	unnel
License	:	AnyConnect Essentials		
Encryption	:	AnyConnect-Parent: (1)r	ione SSL-Tuni	nel: (1)RC4 DTLS-Tunnel: (1)AES128
Hashing	:	AnyConnect-Parent: (1)r	ione SSL-Tuni	nel: (1)SHA1 DTLS-Tunnel: (1)SHA1
Bytes Tx	:	35934	Bytes Rx	: 79714
Group Policy	:	GP-SSL	Tunnel Group	: RA
Login Time	:	17:49:15 CET Sun Mar 16	5 2014	
Duration	:	0h:22m:57s		
Inactivity	:	0h:00m:00s		
VLAN Mapping	:	N/A	VLAN	: none
Audt Sess ID	:	c0a8700a000010005325d60	)b	
Security Grp	:	2:Finance		
Username	:	cisco2	Index	: 2
Assigned IP	:	10.10.11	Public IP	: 192.168.10.80
Protocol	:	AnyConnect-Parent SSL-7	Cunnel DTLS-T	unnel
License	:	AnyConnect Essentials		
Encryption	:	AnyConnect-Parent: (1)r	none SSL-Tuni	nel: (1)RC4 DTLS-Tunnel: (1)AES128
Hashing	:	AnyConnect-Parent: (1)r	none SSL-Tuni	nel: (1)SHA1 DTLS-Tunnel: (1)SHA1
Bytes Tx	:	86171	Bytes Rx	: 122480
Group Policy	:	GP-SSL	Tunnel Group	: RA
Login Time	:	17:52:27 CET Sun Mar 16	5 2014	
Duration	:	0h:19m:45s		
Inactivity	:	0h:00m:00s		
VLAN Mapping	:	N/A	VLAN	: none
Audt Sess ID	:	c0a8700a000020005325d6c	cb	
Security Grp	:	3:Marketing		
SGFW允許微	É貝	オ務(SGT=2)到行銷(SG <sup>™</sup>	「=3)的ICMP》	<sup>而</sup> 量。這就是使用者「cisco」可以ping使用者「
cisco2」的原	Đ		,	

```
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
```

計數增加:

```
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
已建立連線:
```

```
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)
由於已啟用ICMP檢查,因此自動接受返回流量。
```

```
當您嘗試從Marketing(SGT=3)ping Finance(SGT=2)時:
```

#### 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報告:

```
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]
```

### 疑難排解

本節提供的資訊可用於對組態進行疑難排解。

請參閱以下檔案:

• 在Catalyst 3750X系列交換機上使用802.1x MACsec的TrustSec雲配置示例

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

# 摘要

本文給出一個簡單示例,說明如何對VPN使用者進行分類和執行基本實施。SGFW還過濾VPN使用 者與網路其餘部分之間的流量。SXP(TrustSec SGT交換協定)可以在ASA上使用,以獲取IP和 SGT之間的對映資訊。這允許ASA對已正確分類的所有型別的會話(VPN或LAN)執行實施。

在9.2及更高版本的ASA軟體中,ASA還支援RADIUS授權更改(CoA)(RFC 5176)。在成功的VPN狀 態之後,從ISE傳送的RADIUS CoA資料包可以包括cisco-av-pair和SGT,後者將合規使用者分配到 其他(更安全)組。有關更多示例,請參見「相關資訊」部分中的文章。

# 相關資訊

- 採用ISE的ASA 9.2.1版VPN安全評估配置示例
- ASA和Catalyst 3750X系列交換機TrustSec配置示例和故障排除指南
- <u>Cisco TrustSec交換機配置指南:瞭解Cisco TrustSec</u>
- 配置外部伺服器以進行安全裝置使用者授權
- Cisco ASA系列VPN CLI配置指南9.1
- <u>思科身份服務引擎使用手冊,版本1.2</u>
- 技術支援與文件 Cisco Systems

#### 關於此翻譯

思科已使用電腦和人工技術翻譯本文件,讓全世界的使用者能夠以自己的語言理解支援內容。請注 意,即使是最佳機器翻譯,也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準 確度概不負責,並建議一律查看原始英文文件(提供連結)。