PIX/ASA:PPPoE客戶端配置示例

目錄

簡介 必要條件 需求 採用元件 相關產品 慣例 設定 網路圖表 CLI組態 ASDM配置 驗證 清除配置 疑難排解 疑難排解指令 子網掩碼顯示為/32 相關資訊

<u> 簡介</u>

本文檔提供用於版本7.2.(1)及更高版本的ASA/PIX安全裝置作為乙太網點對點協定(PPPoE)客戶端 的配置示例。

PPPoE結合了兩種公認的標準(乙太網和PPP),以提供將IP地址分配給客戶端系統的經過驗證的 方法。PPPoE客戶端通常是通過遠端寬頻連線(例如DSL或電纜服務)連線到ISP的個人電腦。 ISP部署PPPoE是因為它更便於客戶使用,而且它使用現有的遠端訪問基礎設施來支援高速寬頻接 入。

PPPoE提供了一種使用PPPoE網路的身份驗證方法的標準方法。ISP使用時,PPPoE允許對IP地址 進行身份驗證分配。在此類實施中,PPPoE客戶端和伺服器通過運行在DSL或其他寬頻連線上的第 2層橋接協定互連。

PPPoE由兩個主要階段組成:

- 活動發現階段 在此階段, PPPoE客戶端定位一個PPPoE伺服器(稱為訪問集中器),其中 分配了會話ID並建立PPPoE層
- PPP Session Phase 在此階段中,將協商點對點通訊協定(PPP)選項並執行驗證。一旦鏈路 設定完成,PPPoE就充當第2層封裝方法,允許通過PPPoE報頭中的PPP鏈路傳輸資料。

在系統初始化時,PPPoE客戶端會交換一系列資料包,以便與訪問集中器建立會話。建立作業階段 後,會建立PPP連結,此連結使用密碼驗證通訊協定(PAP)進行驗證。建立PPP作業階段後,每個 封包都會封裝在PPPoE和PPP標頭中。 **注意:在**自適應安全裝置上配置故障切換,或在多情景或透明模式下配置故障切換,則不支援 PPPoE。PPPoE僅支援單路由模式,無故障切換。

<u>必要條件</u>

<u>需求</u>

本文件沒有特定需求。

<u>採用元件</u>

本文檔中的資訊基於思科自適應安全裝置(ASA)版本8.x及更高版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路正在作用,請確保您已瞭解任何指令可能造成的影響。

<u>相關產品</u>

此配置還可以與運行7.2(1)及更高版本的Cisco PIX 500系列安全裝置配合使用。為了在Cisco安全 PIX防火牆上配置PPPoE客戶端,PIX OS版本6.2引入了此功能,並且針對低端PIX(501/506)。 有 關詳細資訊,請參閱在Cisco安全PIX防火牆上配置PPPoE客戶端

慣例

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

設定

本節提供設定本檔案中所述功能所需的資訊。

註:使用<u>Command Lookup Tool</u>(僅<u>供</u>已註冊客戶使用)可獲取本節中使用的命令的詳細資訊。

<u>網路圖表</u>

本檔案會使用以下網路設定:



<u>CLI組態</u>

本檔案會使用以下設定:

裝置名稱1

```
ciscoasa#show running-config
: Saved
ASA Version 8.0(2)
1
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
names
1
interface Ethernet0/0
nameif dmz
security-level 50
ip address 10.77.241.111 255.255.255.192
!
interface Ethernet0/1
nameif outside
security-level 0
!--- Specify a VPDN group for the PPPoE client pppoe
client vpdn group CHN
!--- "ip address pppoe [setroute]" !--- The setroute
option sets the default routes when the PPPoE client has
!--- not yet established a connection. When you use the
setroute option, you !--- cannot use a statically
defined route in the configuration. !--- PPPoE is not
supported in conjunction with DHCP because with PPPoE !-
-- the IP address is assigned by PPP. The setroute
option causes a default !--- route to be created if no
default route exists. !--- Enter the ip address pppoe
command in order to enable the !--- PPPoE client from
interface configuration mode.
ip address pppoe
1
interface Ethernet0/2
nameif inside
security-level 100
ip address 10.10.10.1 255.255.255.0
1
interface Ethernet0/3
shutdown
no nameif
no security-level
no ip address
1
interface Management0/0
shutdown
no nameif
no security-level
no ip address
!
passwd 2KFQnbNIdI.2KYOU encrypted
boot system disk0:/asa802-k8.bin
ftp mode passive
access-list 100 extended permit ip any any
access-list inside_nat0_outbound extended permit ip
10.10.10.0 255.255.255.0 10.
20.10.0 255.255.255.0 inactive
pager lines 24
mtu dmz 1500
!--- The maximum transmission unit (MTU) size is
automatically set to 1492 bytes, !--- which is the
```

```
correct value to allow PPPoE transmission within an
Ethernet frame. mtu outside 1492
mtu inside 1500
!--- Output suppressed. global (outside) 1 interface
nat (inside) 1 0.0.0.0 0.0.0.0
!--- The NAT statements above are for ASA version 8.2
and earlier. !--- For ASA versions 8.3 and later the NAT
statements are modified as follows. object network
obj_any
subnet 0.0.0.0 0.0.0.0
nat (inside,outside) dynamic interface
!--- Output suppressed. telnet timeout 5 ssh timeout 5
console timeout 0 !--- Define the VPDN group to be used
for PPPoE. vpdn group CHN request dialout pppoe
!--- Associate the user name assigned by your ISP to the
VPDN group. vpdn group CHN localname cisco
!--- If your ISP requires authentication, select an
authentication protocol. vpdn group CHN ppp
authentication pap
!--- Create a user name and password for the PPPoE
connection. vpdn username cisco password ********
threat-detection basic-threat
threat-detection statistics access-list
!
class-map inspection_default
match default-inspection-traffic
policy-map type inspect dns preset_dns_map
parameters
 message-length maximum 512
policy-map global_policy
class inspection_default
 inspect dns preset_dns_map
 inspect ftp
 inspect h323 h225
 inspect h323 ras
 inspect netbios
 inspect rsh
 inspect rtsp
 inspect skinny
 inspect esmtp
 inspect sqlnet
 inspect sunrpc
 inspect tftp
 inspect sip
 inspect xdmcp
1
service-policy global_policy global
username ciscol23 password ffIRPGpDSOJh9YLq encrypted
privilege 15
prompt hostname context
Cryptochecksum: 3cf813b751fe78474dfb1d61bb88a133
: end
ciscoasa#
```



完成以下步驟,配置隨自適應安全裝置提供的PPPoE客戶端:

註:請參閱<u>允許ASDM進行HTTPS訪</u>問,以便允許ASDM配置ASA。

1. 訪問ASA上的ASDM:開啟瀏覽器,輸入https://<ASDM_ASA_IP_ADDRESS>。其中 ASDM_ASA_IP_ADDRESS是為ASDM訪問配置的ASA介面的IP地址。注意:確保授權瀏覽器 提供的與SSL證書真實性相關的任何警告。預設使用者名稱和密碼均為空。ASA顯示此視窗以 允許下載ASDM應用程式。此示例將應用程式載入到本地電腦上,並且不在Java小程式中運行

Cisco ASDM 6.1
Cisco ASDM 6.1(3) provides an intuitive graphical user interface that makes it easy to set up, configure and manage your Cisco Security Appliances.
Cisco ASDM runs as either a local application or Java Web Start.
Running Cisco ASDM as a local Application When you run Cisco ASDM as a local application, it connects to your Security Appliance from your desktop via SSL. Running Cisco ASDM as an application has these advantages: • You can invoke ASDM from desktop shortcuts. No browser is required. • One desktop shortcut allows you to connect to multiple Security Appliances.
Install ASDM Launcher and Run ASDM
Running Cisco ASDM as Java Web Start
You can run Cisco ASDM as Java Web Start that is dynamically downloaded from the device to which you connect.
Click Run ASDM to run Cisco ASDM.
 Click Run Startup Wizard to run Startup Wizard.Startup Wizard walks you through, step by step, the initial configuration of your security appliance.
Run ASDM Run Startup Wizard

- 2. 按一下Download ASDM Launcher and Start ASDM,下載ASDM應用程式的安裝程式。
- 3. 下載ASDM啟動程式後,完成提示指導的步驟以安裝軟體,然後運行Cisco ASDM啟動程式。
- 4. 輸入您使用http -命令配置的介面的IP地址,如果您指定了一個使用者名稱和密碼。此範例使用 cisco123作為使用者名稱, cisco123作為密碼。

🕵 Cisco ASDM Launch		
	cisco	
Device IP Address / Name:	10.77.241.111	•
Username:	cisco123	
Password:	*****	
🔄 Run in Demo Mode		
	Close	
	. 0	1 🖆

5. 選擇Configuration > Device Setup > Interfaces,突出顯示外部介面,然後按一下Edit。

3

CISCO ASDM 6.1 FOR ASA	- 10.77.241.111	<u>М</u>					کا لگار کا
File View Tools Wizards W	/indow Help	Look For	fi	Dards 🔿	9	Go	duth
Home Sa configuration	Monitoring Sav	e Co Ke	iresn 🔾	васк 🥥	Porward 3	неір	cisco
Device Setup 🗗 🖗 🗡	Configuration > I	Device Se	tup > Inte	rfaces			
	Interface	Name	Enabled	Security Level	IP Address	Subnet M	Add 👻
	Ethernet0/0	dmz	Yes	50	10.77.241.111	255.255.25	Edit
IB A OSPF	Ethernet0/1		No	2			
B B RIP	Ethernet0/2	inside	Yes	100	10.10.10.1	255.255.25	Delete
ELSE ELGRP	Ethernet0/3		No				
Drovy ADDe	Management0/0		No				
System Time System Time Device Setup Firewall	Enable traffic l	between tv	vo or more vo or more	interfaces hosts conn	which are confi lected to the sar	gured with same interface	me security
· LIDES:			Apply		Reset	0	
	CK	co123	15	1		5/11/09 2:	04:42 AM U

- 6. 在Interface Name欄位中,輸入outside,然後選中Enable Interface覈取方塊。
- 7. 按一下IP Address區域中的Use PPPoE單選按鈕。
- 8. 輸入組名稱、PPPoE使用者名稱和密碼,然後按一下相應的PPP身份驗證型別(PAP、 CHAP或MSCHAP)單選按鈕。

a see were on a	Port: Etherne	etD/1		Configure I	Hardware Properties.
Interface I	Jama: outeid				
Internace i	Name. Outside	3			
Security D	evel: U				
Dedica	ate this interfa	e to management only			
Enable	e Interface				
IF AUUres		C			
	Charles The State				
OUse	Static IP	Obtain Address via DHCP	Use PPPoE		
Groun	Name:	Obtain Address via DHCP	Use PPPoE		
Group	Name:	CHN	Use PPPoE		
Group	Name: Username:	Obtain Address via DHCP	Use PPPoE		
Group PPPoE PPPoE	Name: Username: Password:	CHN cisco	Use PPPoE		
Group PPPot PPPot	D Name: Username: Password: rm Password:	Obtain Address via DHCP	Use PPPoE		
Group PPPot PPPot Confir	Name: Username: Password: m Password: wthentication:	Obtain Address via DHCP	Use PPPoE		

9. 按一下**Advanced**頁籤,驗證MTU大小是否設定為**1492。注意:**最大傳輸單元(MTU)大小自動 設定為1492位元組,這是允許乙太網幀內PPPoE傳輸的正確值。

MTU-1492				
Mac Address Clon				
Enter MAC address example 0123.456	ses for the active a 57.89AB).	and standby interfac	es in hexadecimal forma	at (for
Active Mac Addr		Standby Mac Ad	id	

10. 按一下**OK**繼續。

11. 驗證輸入的資訊是否正確,然後按一下Apply。

🚰 Cisco ASDM 6.1 for ASA -	10.77.241.111						,	
File View Tools Wizards Win	dow Help			Look For:			GR	alialia
Home Configuration	Aonitoring 🔚 Sav	e 📿 Ref	fresh 🔇	Back 🔘	Forward 💡 H	ielp		CISCO
Device Setup a P ×	Configuration > I	Device Se	tup > Inte	rfaces				
Startup Wizard	Interface	Name	Enabled	Security Level	IP Address	Subnet Mask	MTU R	Add 🔻
+++ Static Routes	Ethernet0/0	dmz	Yes	50	10.77.241.111	255.255.255	1,500 No	Edit
B 2 OSPF	Ethernet0/1	outside	Yes	0	(PPPoE)	(PPPoE)	1,492 No	
H *A FIGPP	Ethernet0/2	inside	Yes	100	10.10.10.1	255.255.255.0	1,500 No	Delete
Hulticast	Ethernet0/3		No				No	
	<	-					>	
Device Setup	Enable traffic t	oetween tv oetween tv	vo or more vo or more	interfaces hosts conn Apply	which are config ected to the sam	ured with same s ne interface et	ecurity lev	
			ciso	0123	15		5/11/09 2	:09:22 AM UTC



使用本節內容,確認您的組態是否正常運作。

<u>輸出直譯器工具</u>(僅供<u>已註冊</u>客戶使用)(OIT)支援某些**show**命令。使用OIT檢視**show**命令輸出的分析 。

- show ip address outside pppoe 使用此命令以顯示當前PPPoE客戶端配置資訊。
- show vpdn session [l2tp | pppoe] [id sess_id |資料包 |狀態 |視窗] 使用此命令檢視PPPoE會 話的狀態。

以下示例顯示了此命令提供的資訊示例:

hostname#show vpdn Tunnel id 0, 1 active sessions time since change 65862 secs Remote Internet Address 10.0.0.1 Local Internet Address 199.99.99.3 6 packets sent, 6 received, 84 bytes sent, 0 received Remote Internet Address is 10.0.0.1 Session state is SESSION_UP Time since event change 65865 secs, interface outside PPP interface id is 1 6 packets sent, 6 received, 84 bytes sent, 0 received hostname#show vpdn session PPPoE Session Information (Total tunnels=1 sessions=1) Remote Internet Address is 10.0.0.1 Session state is SESSION_UP Time since event change 65887 secs, interface outside PPP interface id is 1

6 packets sent, 6 received, 84 bytes sent, 0 received

hostname#show vpdn tunnel
PPPoE Tunnel Information (Total tunnels=1 sessions=1)
Tunnel id 0, 1 active sessions
 time since change 65901 secs
 Remote Internet Address 10.0.0.1
 Local Internet Address 199.99.99.3
 6 packets sent, 6 received, 84 bytes sent, 0 received
hostname#



要從配置中刪除所有**vpdn group**命令,請在全域性配置模式下使用<u>clear configure vpdn group</u>命令 :

hostname(config)#clear configure vpdn group

若要移除所有vpdn username命令,請使用<u>clear configure vpdn username</u>命令:

hostname(config)#clear configure vpdn username

注意:這些命令對活動的PPPoE連線沒有影響。

<u>疑難排解</u>

<u>疑難排解指令</u>

<u>輸出直譯器工具</u>(僅供<u>已註冊</u>客戶使用)(OIT)支援某些**show**命令。使用OIT檢視**show**命令輸出的分析 。

附註:使用 debug 指令之前,請先參閱<u>有關 Debug 指令的重要資訊</u>。

• hostname# [no] debug pppoe {event |錯誤 | packet} — 使用此命令啟用或禁用PPPoE客戶端的 調試。

子網掩碼顯示為/32

問題

當您使用IP address x.x.x.x 255.255.255.240 pppoe setroute命令時,IP地址分配正確,但子網掩碼 顯示為/32,儘管在命令中將其指定為/28。為什麼會發生這種情況?

解決方案

這是正確的行為。對於PPPoe介面,子網掩碼不相關;asa將始終將其更改為/32。

相關資訊

- <u>Cisco ASA 5500系列調適型安全裝置</u> <u>在Cisco 2600上配置PPPoE客戶端以連線到非Cisco DSL CPE</u>
- 思科調適型資安裝置管理員
- <u>技術支援與文件 Cisco Systems</u>