PIX/ASA Esempio di configurazione del client PPPoE

Sommario

Introduzione **Prerequisiti** Requisiti Componenti usati Prodotti correlati Convenzioni Configurazione Esempio di rete **Configurazione CLI Configurazione ASDM** Verifica Cancellazione della configurazione Risoluzione dei problemi Comandi per la risoluzione dei problemi La subnet mask viene visualizzata come /32 Informazioni correlate

Introduzione

In questo documento viene fornita una configurazione di esempio per l'appliance di sicurezza ASA/PIX come client PPPoE (Point-to-Point Protocol over Ethernet) per le versioni 7.2.2(1) e successive.

PPPoE combina due standard ampiamente accettati, Ethernet e PPP, per fornire un metodo autenticato che assegna indirizzi IP ai sistemi client. I client PPPoE sono in genere personal computer connessi a un ISP tramite una connessione a banda larga remota, ad esempio DSL o un servizio via cavo. Gli ISP implementano il protocollo PPPoE perché è più facile da utilizzare per i clienti e utilizza l'infrastruttura di accesso remoto esistente per supportare l'accesso a banda larga ad alta velocità.

PPPoE fornisce un metodo standard per utilizzare i metodi di autenticazione della rete PPPoE. Se utilizzato dagli ISP, il protocollo PPPoE consente l'assegnazione autenticata di indirizzi IP. In questo tipo di implementazione, il client e il server PPPoE sono interconnessi da protocolli di bridging di layer 2 eseguiti su una connessione DSL o altra connessione a banda larga.

Il PPPoE è costituito da due fasi principali:

• Fase di rilevamento attivo: in questa fase, il client PPPoE individua un server PPPoE,

denominato concentratore di accesso, in cui viene assegnato un ID sessione e viene stabilito il livello PPPoE

• Fase di sessione PPP: in questa fase, le opzioni PPP (Point-to-Point Protocol) vengono negoziate e viene eseguita l'autenticazione. Al termine dell'impostazione del collegamento, il protocollo PPPoE funziona come metodo di incapsulamento di layer 2, che consente il trasferimento dei dati sul collegamento PPP all'interno delle intestazioni PPPoE.

Al momento dell'inizializzazione del sistema, il client PPPoE scambia una serie di pacchetti per stabilire una sessione con il concentratore di accesso. Una volta stabilita la sessione, viene impostato un collegamento PPP che utilizza il protocollo PAP (Password Authentication Protocol) per l'autenticazione. Una volta stabilita la sessione PPP, ogni pacchetto viene incapsulato nelle intestazioni PPPoE e PPP.

Nota: il protocollo PPPoE non è supportato quando il failover è configurato sull'appliance Adaptive Security o in modalità contesto multiplo o trasparente. Il protocollo PPPoE è supportato solo in modalità di routing singolo, senza failover.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Per la stesura del documento, è stata usata la versione 8.x di Cisco Adaptive Security Appliance (ASA) e successive.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Prodotti correlati

Questa configurazione può essere utilizzata anche con Cisco PIX serie 500 Security Appliance, con versione 7.2(1) e successive. Per configurare il client PPPoE su Cisco Secure PIX Firewall, PIX OS versione 6.2 introduce questa funzione ed è destinato ai PIX di fascia bassa (501/506). Per ulteriori informazioni, consultare il documento sulla <u>configurazione del client PPPoE su un firewall Cisco Secure PIX</u>

Convenzioni

Fare riferimento a <u>Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni</u> <u>dei documenti.</u>

Configurazione

In questa sezione vengono fornite le informazioni necessarie per configurare le funzionalità

descritte più avanti nel documento.

Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo <u>strumento di</u> ricerca dei comandi (solo utenti registrati).

Esempio di rete

Nel documento viene usata questa impostazione di rete:



Configurazione CLI

Nel documento vengono usate queste configurazioni:

```
Nome dispositivo 1
ciscoasa#show running-config
: Saved
:
ASA Version 8.0(2)
!
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
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
```

```
interface Ethernet0/2
nameif inside
security-level 100
ip address 10.10.10.1 255.255.255.0
!
interface Ethernet0/3
shutdown
no nameif
no security-level
no ip address
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
1
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#

Configurazione ASDM

Per configurare il client PPPoE fornito con l'appliance di sicurezza adattiva, completare la procedura seguente:

Nota: per consentire all'ASDM di configurare l'appliance ASA, consultare il documento sull'<u>autorizzazione</u> dell'<u>accesso HTTPS per ASDM</u>.

 Accedere all'ASDM sull'appliance ASA: Aprire il browser e immettere https://<ASDM_ASA_IP_ADDRESS>.Dove ASDM_ASA_IP_ADDRESS è l'indirizzo IP dell'interfaccia ASA configurata per l'accesso ASDM.Nota: assicurati di autorizzare gli avvisi che il browser ti invierà relativi all'autenticità del certificato SSL. Il nome utente e la password predefiniti sono entrambi vuoti.L'appliance ASA visualizza questa finestra per consentire il download dell'applicazione ASDM. In questo esempio l'applicazione viene caricata nel computer locale e non viene eseguita in un'applet Java.

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. Per scaricare il programma di installazione dell'applicazione ASDM, fare clic su **Download ASDM Launcher** e su Start ASDM.
- 3. Una volta scaricato l'utilità di avvio ASDM, completare la procedura indicata dalle istruzioni per installare il software ed eseguire l'utilità di avvio Cisco ASDM.
- 4. Immettere l'indirizzo IP per l'interfaccia configurata con il comando http -, nonché un nome utente e una password, se specificati.In questo esempio viene utilizzato cisco123 come nome utente e cisco123 come

	Cisco ASDM Launch		
		cisco	
	Device IP Address / Name:	10.77.241.111	T
	Username:	cisco123	
	Password:	* * * * * * *	
	🔄 Run in Demo Mode		
password		- v	1 🗊 🐇 🔂

5. Scegliete **Configurazione > Impostazione periferica > Interfacce**, evidenziate l'interfaccia esterna e fate clic su

Modifica.

🕵 Cisco ASDM 6.1 for ASA	- 10.77.241.111	1997					
File View Tools Wizards W	indow Help	Look For				Go	ahaha
Home 🍣 Configuration	Monitoring 🔲 Sav	re Ref	fresh 🔾	Back 🜔	Forward ?	Help	CISCO
Device Setup & X	Configuration > I	Device Se	tup > Inte	rfaces			
Startup Wizard	Interface	Name	Enabled	Security Level	IP Address	Subnet M	Add 👻
++++ Static Routes	Ethernet0/0	dmz	Yes	50	10.77.241.111	255.255.25	Edit
B S OSPF	Ethernet0/1		No				
H-A EIGRP	Ethernet0/2	inside	Yes	100	10.10.10.1	255.255.25	Delete
🕀 📲 Multicast	Ethernet0/3		NO				
System Time			1			>	
Evice Setup	Enable traffic l	between tv between tv	vo or more vo or more Apply	interfaces hosts conn	which are conf ected to the sa Reset	igured with sai me interface	me security le
	cis	co123	15			5/11/09 2:	04:42 AM UTC

- 6. Nel campo Nome interfaccia immettere **outside**, quindi selezionare la casella di controllo **Enable Interface**.
- 7. Fare clic sul pulsante di scelta **Usa PPPoE** nell'area Indirizzo IP.
- 8. Immettere un nome di gruppo, un nome utente e una password PPPoE, quindi fare clic sul pulsante di opzione relativo al tipo di autenticazione PPP (PAP, CHAP o MSCHAP).

Lineducere Deets Cheer	antO (1	Confinue Useduase Dranatice
Hardware Fort: Ether	19071	Configure Hardware Properties.
Interface Name: outsi		
Security Level: 0		
Dedicate this interf	ace to management only	
🗹 Enable Interface		
The state of the s		
IP OT FRANCE		
11 Much 635		
Use Static IP () Obtain Address via DHCP 💿 Use PPPoE	
OUse Static IP (Obtain Address via DHCP	
OUse Static IP (Group Name:	Obtain Address via DHCP OUse PPPoE	
Group Name: PPPoE Username:	Obtain Address via DHCP OUse PPPoE	
O Use Static IP (Group Name: PPPoE Username: PPPoE Password:	Obtain Address via DHCP OUse PPPoE	
O Use Static IP (Group Name: PPPoE Username: PPPoE Password: Confirm Password	Obtain Address via DHCP OUse PPPoE CHN cisco	
O Use Static IP (Group Name: PPPoE Username: PPPoE Password: Confirm Password PPP Authentication	Obtain Address via DHCP Use PPPoE	

9. Fare clic sulla scheda Advanced (Avanzate) e verificare che la dimensione MTU sia impostata su 1492.Nota: le dimensioni della MTU (Maximum Transmission Unit) vengono impostate automaticamente su 1492 byte, il valore corretto per consentire la trasmissione PPPoE in un frame

Ethernet.

MTU: 1492				
(
Mac Address Cloning				
Enter MAC addresses example 0123.4567.8	s for the active ar 39AB).	nd standby interface	s in hexadecimal format (for
Active Mac Addr		Standby Mac Add	t	

- 10. Fare clic su **OK** per continuare.
- 11. Verificare che le informazioni immesse siano corrette, quindi fare clic su **Applica**.

Cisco ASDM 6.1 for ASA	- 10.77.241.111							
File View Tools Wizards Wir	ndow Help			Look For:			Q0.	alialis
🔥 Home 😪 Configuration 📴 I	Monitoring 🔚 Sav	e 📿 Ref	fresh 🔇	Back 🜔	Forward 🦻 H	lelp		CISCO
Device Setup ਰਾ 후 ×	Configuration > I	Device Se	tup > Inte	rfaces				0
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
CSPF	Ethernet0/1	outside	Yes	0	(PPPoE)	(PPPoE)	1,492 No	
B-*& FICPP	Ethernet0/2	inside	Yes	100	10.10.10.1	255.255.255.0	1,500 No	Delete
B & Multicast	Ethernet0/3		No				No	-
Device Name/Password	in a lagernaria, o		110					
Device Setup System Time Device Setup System Time	Enable traffic t	between 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	

Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Lo <u>strumento Output Interpreter</u> (solo utenti <u>registrati</u>) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

- **show ip address outside pppoe**: utilizzare questo comando per visualizzare le informazioni di configurazione correnti del client PPPoE.
- show vpdn session [l2tp] | pppoe] [id id_sess | pacchetti | stato | window]: utilizzare questo comando per visualizzare lo stato delle sessioni PPPoE.

Nell'esempio seguente viene illustrato un esempio di informazioni fornite da questo comando:

```
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#
```

Cancellazione della configurazione

Per rimuovere tutti i comandi **vpdn group** dalla configurazione, utilizzare il comando <u>clear</u> <u>configure vpdn group</u> in modalità di configurazione globale:

hostname(config)#clear configure vpdn group

Per rimuovere tutti i comandi vpdn username, usare il comando clear configure vpdn username:

hostname(config)#clear configure vpdn username

Nota: questi comandi non influiscono sulle connessioni PPPoE attive.

Risoluzione dei problemi

Comandi per la risoluzione dei problemi

Lo <u>strumento Output Interpreter</u> (solo utenti <u>registrati</u>) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

Nota: consultare le <u>informazioni importanti sui comandi di debug</u> prima di usare i comandi di **debug**.

 hostname# [no] debug pppoe {event Errore | | packet}: utilizzare questo comando per abilitare o disabilitare il debug per il client PPPoE.

La subnet mask viene visualizzata come /32

Problema

Quando si utilizza il comando **indirizzo IP x.x.x.x 255.255.255.240 pppoe setroute**, l'indirizzo IP viene assegnato correttamente, ma la subnet mask viene visualizzata come /32 sebbene sia specificata nel comando come /28. Perché ciò accade?

Soluzione

Questo è il comportamento corretto. La subnet mask non è pertinente nel caso dell'interfaccia PPPoe; l'ASA la cambia sempre in /32.

Informazioni correlate

- <u>Cisco ASA serie 5500 Adaptive Security Appliance</u>
- Configurazione del client PPPoE su Cisco 2600 per la connessione a un CPE DSL non Cisco
- <u>Cisco Adaptive Security Device Manager</u>
- Documentazione e supporto tecnico Cisco Systems