PIX/ASA: Configuratievoorbeeld van PPPoEclient

Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Verwante producten Conventies Configureren Netwerkdiagram **CLI-configuratie ASDM-configuratie** Verifiëren De configuratie reinigen Problemen oplossen Opdrachten voor probleemoplossing Subnetmasker verschijnt als /32 Gerelateerde informatie

Inleiding

Dit document biedt een voorbeeldconfiguratie voor het ASA/PIX-beveiligingsapparaat als een Point-to-Point Protocol over Ethernet (PPPoE)-client voor versies 7.2.2(1) en hoger.

PPPoE combineert twee breed geaccepteerde standaarden, Ethernet en PPP, om een geauthentiseerde methode te voorzien die IP adressen aan clientsystemen toewijzen. PPPoEclients zijn doorgaans persoonlijke computers die via een externe breedbandverbinding op een ISP zijn aangesloten, zoals DSL of kabelservice. ISP's zetten PPPoE op omdat het voor klanten gemakkelijker is om te gebruiken en zij gebruikt hun bestaande infrastructuur voor externe toegang om snelle breedbandtoegang te ondersteunen.

PPPoE verstrekt een standaardmethode om de authenticatiemethoden van het PPPoE-netwerk aan te wenden. Wanneer het door ISP's wordt gebruikt, staat PPPoE een authenticatie van de IPadressen toe. In dit type implementatie, worden de client PPPoE en de server onderling verbonden door Layer 2 overbruggingsprotocollen die over een DSL of andere breedbandverbinding lopen.

PPPoE bestaat uit twee hoofdfasen:

• Actieve de Fase-In deze fase, plaats de client PPPoE een PPPoE-server, genoemd een

toegangsconcentrator, waar een sessie-ID wordt toegewezen en de laag PPPoE wordt gevestigd

• PPP Session fase-In deze fase worden Point-to-Point Protocol (PPP)-opties onderhandeld en wordt verificatie uitgevoerd. Zodra de installatie van de link is voltooid, werkt PPPoE als een Layer 2-insluitingsmethode, waarmee gegevens via de PPP-link binnen PPPoE-headers kunnen worden overgedragen.

Bij systeeminitialisatie, ruilt de PPPoE client een reeks pakketten om een sessie met de toegangsconcentrator op te zetten. Zodra de sessie wordt vastgesteld, wordt een PPP-link ingesteld, die Wachtwoord Verificatieprotocol (PAP) gebruikt voor verificatie. Zodra de PPP-sessie wordt vastgesteld, wordt elk pakje ingesloten in de PPPoE- en PPP-headers.

Opmerking: PPPoE wordt niet ondersteund wanneer failover is geconfigureerd op het adaptieve security apparaat, of in meerdere context of transparante modus. PPPoE wordt alleen ondersteund in enkele, routemodus, zonder failover.

<u>Voorwaarden</u>

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op versie 8.x van Cisco adaptieve security applicatie (ASA) en hoger.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Verwante producten

Deze configuratie kan ook worden gebruikt met de Cisco PIX 500 Series security applicatie, die versie 7.2(1) en hoger uitvoeren. Om de PPPoE-client te configureren op de Cisco Secure PIX-firewall, introduceert PIX OS-versie 6.2 deze functie en is gericht op de low-end PIX (501/506). Raadpleeg voor meer informatie <u>het configureren van de PPPoE-client op een Cisco Secure PIX-firewall</u>

Conventies

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

Configureren

Deze sectie verschaft de informatie die nodig is om de functies te configureren die in dit document worden beschreven.

Opmerking: Gebruik het <u>Opname Gereedschap</u> (<u>alleen geregistreerde</u> klanten) om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.

Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:



CLI-configuratie

Dit document gebruikt deze configuraties:

```
Apparaatnaam 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
!
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
1
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
!
service-policy global_policy global
username ciscol23 password ffIRPGpDSOJh9YLq encrypted
privilege 15
prompt hostname context
Cryptochecksum:3cf813b751fe78474dfb1d61bb88a133
: end
ciscoasa#

ASDM-configuratie

Voltooi deze stappen om de PPPoE-client te configureren die met het adaptieve security apparaat wordt meegeleverd:

Opmerking: Raadpleeg <u>HTTPS-toegang voor ASDM</u> om de ASA te kunnen configureren door de ASDM.

1. Toegang tot ASDM op de ASA:Open uw browser en voer

https://<ASDM_ASA_IP_ADDRESS>in.Waar ASDM_ASA_IP_ADRESS het IP-adres is van de ASA-interface die is geconfigureerd voor ASDM-toegang.Opmerking: Controleer of u een waarschuwing geeft die uw browser aan SSL-certificaat en de authenticiteit ervan geeft. De standaard naam en het wachtwoord zijn beide leeg.ASA geeft dit venster weer om de ASDM-toepassing te kunnen downloaden. Dit voorbeeld laadt de toepassing op de lokale computer en werkt niet in een Java-

applet.

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.						
 When you run 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 <i>multiple</i> 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. Klik op **Download ASDM Launcher en Start ASDM** om de installateur voor de ASDMtoepassing te downloaden.
- 3. Nadat de ASDM Launcher is gedownload, voltooit u de stappen die door de aanwijzingen zijn geleid om de software te installeren en de Cisco ASDM Launcher uit te voeren.
- 4. Voer het IP-adres in voor de interface die u met de http-opdracht hebt ingesteld en indien u er een hebt opgegeven, een naam en een wachtwoord.Dit voorbeeld gebruikt **cisco123** voor de gebruikersnaam en **cisco123** als het

ៅ Cisco ASDM Launch	er v1.5(30)				
	cisco				
Device IP Address / Name:	10.77.241.111	T			
Username:	cisco123				
Password:	****				
📃 Run in Demo Mode					
	. 0	📋 👙 🔒			

wachtwoord.

5. Kies **Configuratie > Instellen apparaat > Interfaces**, markeer de externe interface en klik op **Bewerken**.

	10.77.241.111						النارح
File View Tools Wizards Wir Home 🍣 Configuration 📴 !	ndow Help Monitoring 📊 Sav	Look For	resh 🔇	Back 🔘	Forward 🦻 H	telp	dindin cisco
Device Setup 🗗 🖗 🗙	Configuration > I	Device Se	tup > Inte	rfaces			0
Startup Wizard	Interface	Name	Enabled	Security Level	IP Address	Subnet M	Add 👻
-+	Ethernet0/0	dmz	Yes	50	10.77.241.111	255.255.25	Edit
0SPF	Ethernet0/1		No				
B the RIP	Ethernet0/2	inside	Yes	100	10.10.10.1	255.255.25	Delete
ELGRP	Ethernet0/3		No				
Provy APPe	Management0/0		No				
# 🧿 System Time						>	
Device Setup	Enable traffic l	oetween tv oetween tv	vo or more	interfaces hosts conn	which are config ected to the sar	jured with san	ne security

- 6. Typ buiten in het veld Naam interface en controleer het vakje Interface inschakelen.
- 7. Klik het radioknop Gebruik PPPoE in het IP adresgebied.
- Voer een groepsnaam, PPPoE-gebruikersnaam en wachtwoord in en klik op de juiste PPPverificatietype (PAP, CHAP of MSCHAP).

Hardware Port: Ethern	et0/1	Configure Hardware Properties.
Interface Name: outsid	e	
Security Level: 0]	
Dedicate this interfa	ce to management only	
Enable Interface		
Group Name:	CHN	
PPPoE Lisername	cisco	
The open ane.		
PPPoE Password:		
PPPoE Password: Confirm Password:	•••••	
PPPoE Password: Confirm Password: PPP Authentication		

9. Klik op het tabblad Geavanceerd en controleer of de grootte van de MTU is ingesteld op 1492.Opmerking: De maximale grootte van een transmissieeenheid (MTU) wordt automatisch ingesteld op 1492 bytes. Dit is de juiste waarde om PPPoE-transmissie binnen een Ethernet-frame toe te staan.

MTU: 1492		
<u> </u>		
Mac Address Cloning	ng	
Enter MAC addresse example 0123.4567.	es for the active and standby interfaces in hexadecimal format (fo '.89AB).	or
Active Mac Addr	Standby Mac Add	

- 10. Klik op **OK** om verder te gaan.
- 11. Controleer dat de informatie die u hebt ingevoerd, juist is en klik op **Toepassen**.

🖆 Cisco ASDM 6.1 for ASA -	10.77.241.111							
File View Tools Wizards Win	idow Help Aonitoring 🕞 Sav	e 📿 Ref	fresh 🔇	Look For: Back 🚫	Forward 🤋 H	lelp	60	cisco
Device Setup ਰਾ 후 ×	Configuration > I	Device Se	tup > Inte	rfaces				0
- 5 ⁹ Startup Wizard - 5 ¹⁰ Interfaces - 4 ³ Routing	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
COPF	Ethernet0/1	outside	Yes	0	(PPPoE)	(PPPoE)	1,492 No	
B-16 RIP	Ethernet0/2	inside	Yes	100	10.10.10.1	255.255.255.0	1,500 No	Delete
Multicast	Ethernet0/3		No				No	
a V System nime								
	<						>	
Device Setup	Enable traffic t	oetween tv	vo or more vo or more	interfaces hosts conn Apply	which are config ected to the san	ured with same s ne interface et	ecurity lev	
			ciso	0123	15	i i i i i i i i i i i i i i i i i i i	5/11/09 2	:09:22 AM UTC

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Het <u>Uitvoer Tolk</u> (<u>uitsluitend geregistreerde</u> klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.

- toon ip adres buiten PPPoE gebruik deze opdracht om de huidige PPPoE client configuratieinformatie weer te geven.
- VPN-sessie tonen [l2tp | ppo's [id sess_id] | Verpakking | Staat | venster]—gebruik deze opdracht om de status van PPPoE-sessies te bekijken.

Het volgende voorbeeld toont een voorbeeld van informatie die door deze opdracht wordt verstrekt:

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#
```

De configuratie reinigen

Om alle opdrachten van **de vpdn groep** uit de configuratie te verwijderen, gebruikt u de opdracht <u>duidelijk</u> de <u>configuratie van de VPDN-groep</u> in de wereldwijde configuratie-modus:

hostname(config)#clear configure vpdn group

Om alle **VPDN-**opdrachten te verwijderen, gebruikt u de <u>duidelijke</u> opdracht<u>van de</u> gebruikersnaam<u>voor configuratie vpdn</u>:

hostname(config)#clear configure vpdn username

Opmerking: deze opdrachten hebben geen invloed op actieve PPPoE-verbindingen.

Problemen oplossen

Opdrachten voor probleemoplossing

Het <u>Uitvoer Tolk</u> (<u>uitsluitend geregistreerde</u> klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.

Opmerking: Raadpleeg <u>Belangrijke informatie over debug Commands</u> voordat u **debug**opdrachten gebruikt.

• hostname# [no] debug van pop {event] | vergissing | pakket —gebruik deze opdracht om het foutoptreden voor de PPPoE-client in te schakelen of uit te schakelen.

Subnetmasker verschijnt als /32

Probleem

Wanneer u het **IP-adres x.x.x.x 255.255.255.240 ppo** bevel gebruikt, wordt het IP-adres correct toegewezen, maar het subnetmasker verschijnt als /32 alhoewel het in de opdracht als /28 wordt gespecificeerd. Waarom gebeurt dit?

Oplossing

Dit is het juiste gedrag. Het subnetmasker is irrelevant in het geval van de PPPoe-interface; de ASA zal dit altijd veranderen in /32.

Gerelateerde informatie

- <u>Cisco ASA 5500 Series adaptieve security applicaties</u>
- PPPoE-client configureren op Cisco 2600 om verbinding te maken met een niet-Cisco DSL CPE
- <u>Cisco adaptieve security apparaatbeheer</u>
- Technische ondersteuning en documentatie Cisco Systems