PIX/ASA : Groepen van Kerberos-verificatie en LDAP-licentieservers voor VPN-clientgebruikers via het configuratievoorbeeld ASDM/CLI

Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Verwante producten Conventies Achtergrondinformatie Verificatie en autorisatie voor VPN-gebruikers configureren met ASDM Verificatie- en licentieservers configureren Een VPN-tunnelgroep configureren voor verificatie en autorisatie Verificatie en autorisatie voor VPN-gebruikers configureren met CLI Verificatie en autorisatie voor VPN-gebruikers configureren met CLI Verifiëren Problemen oplossen Gerelateerde informatie

Inleiding

Dit document beschrijft hoe u de Cisco Adaptieve Security Devices Manager (ASDM) kunt gebruiken om Kerberos-verificatie en de LDAP-servergroepen te configureren op de Cisco PIX 500 Series security applicatie. In dit voorbeeld worden de servergroepen door het beleid van een VPN tunnelgroep gebruikt om binnenkomende gebruikers voor de authenticatie en autorisatie te zorgen.

Voorwaarden

Vereisten

In dit document wordt ervan uitgegaan dat de PIX volledig gebruiksklaar is en is geconfigureerd om ASDM in staat te stellen de configuratie te wijzigen.

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

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco PIX security applicatie, versie 7.x en hoger
- Cisco ASDM versie 5.x 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 Cisco adaptieve security applicatie (ASA) versie 7.x.

Conventies

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

Achtergrondinformatie

Niet alle mogelijke verificatie- en autorisatiemethoden die in de PIX/ASA 7.x-software beschikbaar zijn, worden ondersteund wanneer u met VPN-gebruikers omgaat. In deze tabel wordt uitgelegd welke methoden beschikbaar zijn voor VPN-gebruikers:

	Loka al	RADI US	TACAC S+	SD I	NT	Kerber os	LDA P
Verificatie	Ja	Ja	Ja	Ja	Ja	Ja	Nee
Authorizat ion	Ja	Ja	Nee	Ne e	Ne e	Nee	Ja

Opmerking: Kerberos wordt gebruikt voor de authenticatie en LDAP wordt gebruikt voor de autorisatie van VPN-gebruikers in dit voorbeeld.

Verificatie en autorisatie voor VPN-gebruikers configureren met ASDM

Verificatie- en licentieservers configureren

Voltooi deze stappen om verificatie- en autoriteitsservergroepen voor VPN-gebruikers te configureren via ASDM.

1. Kies Configuratie > Eigenschappen > AAA Instellingen > AAA-servergroepen en klik op Toevoegen.

Cisco ASDM !	5.0 for PIX - 10.89.129.147					
File Rules 3	earch Options Tools Wizards	Help				
<h></h>	- A - A - A - A - A - A - A - A - A - A	00	\bigcirc $ $ \bigcirc	ا ا	2	CISCO SYSTEMS
Home	Configuration Monitoring	Back Forward	Search Refre	sh Save H	elp	միկտ։։
Features	Configuration > Features > Prop	renties > AAA Bebup > AA	A Berver Groups			
	● 全革 ■ 前 太 助					
	Et 🚽 AAA Sebup	AAA Server Groups				
Interfaces	AAA Server Grou	Continue 610 course				
6	AAA Servers	each group. Individua	groups and the p il servers must bi	configured for extern	ni use to communicate with hal groups.	
Security Policy	- Auth. Prompt				in grouper	
8.4	E- Calabianced	Server Group	Protocol	Accounting Mode	Reactivation Mode	D Add
64		LOCAL	LOCAL			E-da
NAT	- TCP Options					
<u> </u>	- O Timeouts					Delete
VPN	- ARP Static Table					
436	Et & DHCP Benices					
240 Economic	- MOHOP Server					
room g	- PDHCP Relay					
8	DNS Client					
Building Blocks	Fallover					
<u></u>	- M History Metrics					
Device	- Paulit Policy					
Administration	🗆 😼 IP Audit Signatur					
2.	E 🔁 Logging					
Properties						
	Event Lists					•
	Syslog Setup					
	-En Syslog Servers		P	pply F	Reset	
Wizards - <						
			cisco	NA (15)	000 1/1 🔂 📋 📕	6 10:32:03 PM UT(

2. Defineer een naam voor de nieuwe groep van de authentificatieserver, en kies een protocol.De optie Accounting Mode is alleen voor RADIUS en TACACS+. Klik op **OK** wanneer u klaar



3. Herhaal stap 1 en 2 om een nieuwe autorisatieserver te

1	🔂 Add AAA Server Gro	up		×
	Configure AAA server (applicable for RADIUS	group. The Accounting and TACACS+ protoco	Mode attribute is only ols.	
	Server Group:	my_author_grp		
	Protocol:	LDAP	•	
	Accounting Mode:	C Simultaneous	 Single 	
	Reactivation Mode:	Depletion	C Timed	
	Dead Tin	ne: 10	minutes	
	Max Failed Attempts:	3		
	OK	Cancel	Help	
maken		A		

4. Klik op **Toepassen** om de wijzigingen in het apparaat door te sturen.



Als u dit zo hebt ingesteld, presteert het apparaat nu de opdrachten die aan de actieve configuratie zijn toegevoegd.

5. Klik op **Verzend** de opdrachten naar het apparaat.

hanges in ASDM, click Cancel.	click Send. To not send the commands and continue ma	aking
aaa-server my_authent_grp aaa-server my_authent_grp reactivation-mode depletior max-failed-attempts 3 aaa-server my_author_grp p aaa-server my_author_grp p reactivation-mode depletior max-failed-attempts 3	protocol kerberos protocol kerberos n deadtime 10 protocol Idap protocol Idap n deadtime 10	

VI.

De nieuw gecreëerde servergroepen moeten nu worden bevolkt met authenticatie- en autorisatieservers.

6. Kies Configuration > Properties > AAA Setup > AAA servers en klik op Add.



7. Configureer een verificatieserver. Klik op OK wanneer u klaar

🛓 Add AAA Server							×
Server Group:		my_auth	ent_grp			•	
Interface Name:		inside				•	
Server IP Address:		172.22.1	.100				
Timeout:		10		secon	ds		
– Kerberos Parame	ters						
Server Port:	88						
Server Port: Retry Interval:	88 10 second	Is				•	
Server Port: Retry Interval: Kerberos Realm:	88 10 second REALM.CI	Is SCO.COM				•	
Server Port: Retry Interval: Kerberos Realm:	88 10 second REALM.CI	Is SCO.COM				•	
Server Port: Retry Interval: Kerberos Realm:	88 10 second REALM.CI	Is SCO.COM				•	
Server Port: Retry Interval: Kerberos Realm:	88 10 second REALM.CI	Is SCO.COM				•	
Server Port: Retry Interval: Kerberos Realm:	88 10 second REALM.CI	Is SCO.COM				•	
Server Port: Retry Interval: Kerberos Realm:	88 10 second REALM.CI	Is SCO.COM		Holp		•	

roep - Kies de servergroep voor de verificatie die in stap 2 is ingesteld.**Interface Naam** - Kies de interface waarop de server zich bevindt.**IP-adres van de server**-Specificeer het IP-adres van de verificatieserver.**Time-out**-Specificeer de maximale tijd, in seconden, om te wachten op een reactie van de server.**Kerberos-parameters:Server Port**-88 is de standaardpoort voor Kerberos.**Interval opnieuw proberen**—Kies het gewenste interval.**Kerberos Realm**-Voer de naam van uw Kerberos gebied in. Dit is vaak de Windows-domeinnaam in alle hoofdletters.

8. Configureer een server. Klik op \mathbf{OK} na

🔂 Add AAA Server	X
Server Group:	my_author_grp
Interface Name:	inside
Server IP Address:	172.22.1.101
Timeout:	10 seconds
LDAP Parameters	
Server Port:	389
Base DN:	ou=cisco
Scope:	One level beneath the Base DN
Naming Attribute(s):	uid
Login DN:	
Login Password:	
Confirm Login Password:	
ок 🖓 –	Cancel Help

voltooiing.

rvergroep - Kies de autoriseservergroep die in stap 3 is ingesteld.**Interface Naam** - Kies de interface waarop de server zich bevindt.**IP-adres van de server**-Specificeer het IP-adres van de licentieserver.**Time-out**-Specificeer de maximale tijd, in seconden, om te wachten op een reactie van de server.**LDAP-parameters:Server Port**—389 is de standaardpoort voor LDAP.**Base DN**-Voer de locatie in de LDAP-hiërarchie in waar de server moet beginnen met zoeken nadat het een vergunningsaanvraag heeft ontvangen.**Toepassingsgebied** - Kies in welke mate de server de LDAP-hiërarchie moet doorzoeken zodra de server een vergunningsaanvraag heeft ontvangen.**Namingkenmerk(en)**—Voer de relatieve onderscheidende eigenschap(pen) van de naam in waardoor de items op de LDAP-server uniek zijn gedefinieerd. Vaak voorkomende naamgevingseigenschappen zijn veelvoorkomende naam (cn) en gebruiker-ID (uid).**Login DNA**-Sommige LDAP-servers, inclusief de Microsoft Active Directory-server, vereisen dat het apparaat een handdruk opstelt via een geauthentiseerde binding voordat ze aanvragen voor andere LDAP-bewerkingen

aanvaarden. Het veld Login DN definieert de echtheidskenmerken van het apparaat, die corresponderen met die van een gebruiker met administratierechten. Bijvoorbeeld, cn=beheerder. Laat dit veld leeg voor anonieme toegang.**Login Wachtwoord**-Voer het wachtwoord in voor de Aanmelden-DNA.**Bevestig Login Wachtwoord** - Bevestig het wachtwoord voor de Aanmelden-DNA.

- 9. Klik op **Toepassen** om de wijzigingen in het apparaat door te sturen nadat alle verificatie- en autorisatieservers zijn toegevoegd. Als u dit zo hebt ingesteld, wordt in PIX nu de opdrachten gepresteerd die aan de actieve configuratie worden toegevoegd.
- 10. Klik op Verzend de opdrachten naar het apparaat.

Een VPN-tunnelgroep configureren voor verificatie en autorisatie

Voltooi deze stappen om de servergroepen toe te voegen die u zojuist hebt ingesteld voor een VPN-tunnelgroep.

 Kies Configuration > VPN > Tunnel Group en klik op Add om een nieuwe tunnelgroep te maken of Bewerken om een bestaande groep te wijzigen

wijzigen.					
Ella Rirlas Ba	0 for PIX - 10.89.129.147 arch Ontions Tools Witzerds	e Hain			_ O ×
Home G	Configuration Monitoring	Back Forward Search	Refresh Save	? Help	Cisco Systems
Features	Configuration > Features > VPI	N > General > Tunnel Group			
Interfaces	⊕ ⊕ ⊕	A III. III. III. III. III. Tunnel Group Manage VPN tunnel grou IPSec connections.	ips. A VPN tunnel group i	represents a connection sp	ecific record for
in the second		Name	Туре	Group Policy	Add
NAT	Price Set State Set Set Set Set Set Set Set Set Set S	DefaultRAGroup DefaultL2LGroup	ipsec-ra ipsec-121	DftGrpPolicy DftGrpPolicy	Edit
Administration Properties	L @IP Pools	Specify the delimeter to b are received when tunnel Group Delimiter:	e used when parsing fur s are being negotiated. one 💌	nnel group names from the Reset	user name that
THZarus A	· ·		lcisco INA (15)		LTR 906 10 46 03 PM UT
			0.000 100(10)	29 23	1/13/00 T0.46.03 PMF0TC

2. Selecteer in het tabblad General van het venster dat nu wordt weergegeven de servergroepen die eerder zijn ingesteld.

🔂 Add Tunnel Group
Identity General Client Address Assignment IPSec Advanced
Group Policy: DfltGrpPolicy
Strip the realm from username before passing it on to the AAA server
Strip the group from username before passing it on to the AAA server
To set authentication server group per interface, go to the Advanced tab.
Authentication Server Group: my_authent_grp
Use LOCAL if Server Group fails
Authorization Server Group: my_author_grp
Users must exist in the authorization database to connect
Accounting Server Group: None
OK Cancel Help

- 3. *Optioneel:* Configureer de resterende parameters op de andere tabbladen als u een nieuwe tunnelgroep toevoegt.
- 4. Klik op **OK** wanneer u klaar bent.
- 5. Klik op **Toepassen** om de wijzigingen in het apparaat door te sturen nadat de configuratie van de tunnelgroep is voltooid.Als u dit zo hebt ingesteld, wordt in PIX nu de opdrachten gepresteerd die aan de actieve configuratie worden toegevoegd.
- 6. Klik op Verzend de opdrachten naar het apparaat.

Verificatie en autorisatie voor VPN-gebruikers configureren met CLI

Dit is de equivalente CLI-configuratie voor de verificatie- en autorisatie servergroepen voor VPNgebruikers.

Configuratie van security applicatie CLI

```
pixfirewall#show run
: Saved
:
PIX Version 7.2(2)
!
hostname pixfirewall
domain-name default.domain.invalid
enable password 8Ry2YjIyt7RRXU24 encrypted
names
1
interface Ethernet0
 shutdown
no nameif
no security-level
no ip address
!
interface Ethernet1
nameif inside
security-level 100
ip address 172.22.1.105 255.255.255.0
!
!--- Output is suppressed. ! passwd 2KFQnbNIdI.2KYOU
encrypted ftp mode passive dns server-group DefaultDNS
domain-name default.domain.invalid pager lines 24 mtu
inside 1500 no failover icmp unreachable rate-limit 1
burst-size 1 asdm image flash:/asdm-522.bin !--- Output
is suppressed. aaa-server my_authent_grp protocol
kerberos
aaa-server my_authent_grp host 172.22.1.100
kerberos-realm REALM.CISCO.COM
aaa-server my_author_grp protocol ldap
aaa-server my_author_grp host 172.22.1.101
ldap-base-dn ou=cisco
 ldap-scope onelevel
ldap-naming-attribute uid
http server enable
http 0.0.0.0 0.0.0.0 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup
linkdown coldstart
tunnel-group DefaultRAGroup general-attributes
authentication-server-group my_authent_grp
authorization-server-group my_author_grp
!--- Output is suppressed.
```

Verifiëren

Voltooi deze stappen om de gebruikersverificatie tussen de PIX/ASA- en AAA-server te controleren:

 Kies Configuration > Properties > AAA Setup > AAA servers en selecteer de servergroep (my_authent_grp). Klik vervolgens op Test om de gebruikersreferenties te valideren.

📬 Cisco ASDM 5	0 for PIX - 10.89.129.147					_10
File Rules Se	arch Options Tools Wizard	is Help				
di Home	Configuration Monitoring	Back Forward	d Search F	💽 🔜 Refresh Save	? Help	Cisco Syste
Features	Configuration = Features > Pr	operties > AAA Setu	p > AAA Servers			
	● 全等 ■ 前 氷	54 18 16 19 14	ă I			
Interfaces	AAA Setup	AAA Servers Add and configu go to the <u>AAA Se</u>	ire AAA servers for ever Groups scree	existing AAA server n.	groups. To configure s	erver groups
Security Policy	🕀 🐻 Advanced	Server Gr	roup (Protocol)	Interface	Server IP Address	Timeout Hed
NAT	- Spoofing - Spoofing - Spoofing - Spoofing - Spoofing	my_authe	nt_grp	inside	172.22.1.100	10
VPN VPN	💮 Timeouts 🛲 ARP Static Table 🌉 Auto Update					Tesix
420	E PDHCP Services					10012
Routing	- PDHCP Sarver - PDHCP Relay - ■DNS Client					\smile
Building Blocks	Failover					

2. Geef de gebruikersnaam en het wachtwoord op (bijvoorbeeld de gebruikersnaam: test en wachtwoord: test), en klik op **OK** om te

	🚰 Test AAA Server -172.	.22.1.100
	To test the following AA password.	A server enter username and
	AAA Server Group:	my_authent_grp (Kerberos)
	Host:	172.22.1.100
	${f C}$ Authorization	Authentication
	Username:	test
	Password:	***
valideren.	ок	Cancel

3. U kunt zien dat de Verificatie succesvol



Problemen oplossen

- Eén frequente oorzaak van echtheidsfalen is klokscheefheid. Zorg ervoor dat de klokken op de PIX- of ASA- en uw verificatieserver gesynchroniseerd zijn.Wanneer verificatie niet werkt vanwege klokscheefheid, kunt u deze foutmelding ontvangen: -- FOUT: Verificatie
 verworpen: Klokscheefheid groter dan 300 seconden.. Dit logbericht verschijnt ook:%PIX|ASA-3-113020: Kerberos-fout: Klokscheefheid met ip_adres van de server is groter dan 300 seconden ip_adres— Het IP adres van de Kerberos server.Dit bericht wordt weergegeven wanneer de verificatie voor een IPSec- of WebVPN-gebruiker door een Kerberos-server mislukt, omdat de klokken op het security apparaat en de server meer dan vijf minuten (300 seconden) uit elkaar liggen. Wanneer dit voorkomt, wordt de verbindingspoging verworpen.Om dit probleem op te lossen, synchroniseert u de klokken op het security apparaat en de Kerberos server.
- 2. Verificatie vooraf in de Active Directory (AD) moet worden uitgeschakeld, of dit kan leiden tot een storing van de gebruikersverificatie.
- 3. VPN-clientgebruikers kunnen zich niet aanmelden tegen de Microsoft certificaatserver. Dit foutbericht verschijnt:"Fout bij verwerken van lading" (fout 14) Om deze kwestie op te lossen, uncheck de machine **niet kerberose preauthenticatie** selectieteken op de authenticatieserver **vereist**.

Gerelateerde informatie

- AAA-servers en de lokale database configureren
- <u>Cisco ASA 5500 Series productondersteuning voor adaptieve security applicaties</u>
- <u>Cisco PIX-firewallsoftware</u>
- Opdrachtreferenties van Cisco Secure PIX-firewall
- Security meldingen uit het veld (inclusief PIX)
- Verzoeken om opmerkingen (RFC's)
- <u>Technische ondersteuning en documentatie Cisco Systems</u>