PIX/ASA: Esempio di configurazione dell'autenticazione Kerberos e dei gruppi di server di autorizzazione LDAP per utenti client VPN tramite ASDM/CLI

Sommario

Introduzione Prerequisiti Requisiti Componenti usati Prodotti correlati Convenzioni Premesse Configurazione dell'autenticazione e dell'autorizzazione per gli utenti VPN tramite ASDM Configura server di autenticazione e autorizzazione Configurare un gruppo di tunnel VPN per l'autenticazione e l'autorizzazione Configurazione dell'autenticazione e dell'autorizzazione per gli utenti VPN tramite CLI Verifica Risoluzione dei problemi Informazioni correlate

Introduzione

In questo documento viene descritto come usare Cisco Adaptive Security Device Manager (ASDM) per configurare i gruppi di server di autenticazione Kerberos e autorizzazione LDAP sull'appliance di sicurezza Cisco PIX serie 500. In questo esempio, i gruppi di server vengono utilizzati dai criteri di un gruppo di tunnel VPN per autenticare e autorizzare gli utenti in ingresso.

Prerequisiti

Requisiti

In questo documento si presume che il PIX sia completamente operativo e configurato per consentire all'ASDM di apportare modifiche alla configurazione.

Nota: per consentire la configurazione del PIX da parte di ASDM, consultare il documento sulla <u>concessione</u> dell'<u>accesso HTTPS</u> per ASDM.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Software Cisco PIX Security Appliance versione 7.x e successive
- Cisco ASDM versione 5.x 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 Adaptive Security Appliance (ASA) versione 7.x.

Convenzioni

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

Premesse

Non tutti i possibili metodi di autenticazione e autorizzazione disponibili nel software PIX/ASA 7.x sono supportati quando si ha a che fare con utenti VPN. In questa tabella vengono descritti i metodi disponibili per gli utenti VPN:

	Loca le	RAGG IO	TACAC S+	S DI	N T	Kerber os	LDA P
Autenticazi one	Sì	Sì	Sì	Sì	Sì	Sì	No
Authorizati on	Sì	Sì	No	N o	N o	No	Sì

Nota: Kerberos viene utilizzato per l'autenticazione e LDAP per l'autorizzazione degli utenti VPN in questo esempio.

Configurazione dell'autenticazione e dell'autorizzazione per gli utenti VPN tramite ASDM

Configura server di autenticazione e autorizzazione

Completare questa procedura per configurare i gruppi di server di autenticazione e autorizzazione per gli utenti VPN tramite ASDM.

 Scegliere Configurazione > Proprietà > Impostazione AAA > Gruppi di server AAA, quindi fare clic su Aggiungi.

Cisco ASDM S	5.0 for PIX - 10.89.129.147					
File Rules S	earch Options Tools Wizards	Help				
C Home	Configuration Monitoring	Back Forward	Q G Search Refr	ish Save H	?	Cisco Systems
Features	Configuration > Features > Prop	perties > AAA Setup > AA	A Berver Groups			
Interfaces	⊕	A R. R. R. R. Coups AAA Server Groups Configure AAA server each group. Individua	groups and the p I servers must b	rotocols the device w e configured for extern	III use to communicate with nal groups.	
	E- SAdvanced	Server Group	Protocol	Accounting Mode	Reactivation Mode 0	Add N
NAT	- Spooting	LOCAL	LOCAL			Edit
	- Timeouts - ARP Static Table - Auto Update					Delete
430	🗄 🚰 DHCP Services					
Routing	- PDHCP Server					
0	- P DHCP Relay					
8 8	DNS Client					
Building Blocks	- Mictory Matrice					
- <u>- </u>	P IP Audi					
Device	- Pill P Audit Policy					
Administration	- 🧟 IP Audit Signatur					
	🕀 🛅 Logging					
Properties						
	F-ttl Event Lists	1			,	1
	Sysing Setup					-
	- Syslog Servers		P	vige:	Reset	
Wizards /	I I Mensor					
	,		cisco	NA (15)	 0001111100	6 10:32:03 PM UTC

2. Definire un nome per il nuovo gruppo di server di autenticazione e scegliere un protocollo.L'opzione Modalità accounting è disponibile solo per RADIUS e TACACS+. Al termine, fare clic su



3. Ripetere i passaggi 1 e 2 per creare un nuovo gruppo di server di autorizzazione.

🚰 Add AAA Server Group 🛛 🔀					
Configure AAA server group. The Accounting Mode attribute is only applicable for RADIUS and TACACS+ protocols.					
Server Group:	my_author_grp				
Protocol:	LDAP				
Accounting Mode:	C Simultaneous 💿 Single				
Reactivation Mode:	Depletion O Timed				
Dead Tin	ne: 10 minutes				
Max Failed Attempts:	3				
ОК	Cancel Help				

4. Per inviare le modifiche al dispositivo, fare clic su **Apply** (Applica).



Se è stato configurato per tale operazione, il dispositivo visualizza ora in anteprima i comandi aggiunti alla configurazione in esecuzione.

5. Per inviare i comandi al dispositivo, fare clic su **Send**.

review CLI Commands			
The following CLI commands are send the commands to the PIX, c changes in ASDM, click Cancel.	generated based on the char lick Send. To not send the cor	nges you made in ASDM. To mmands and continue making	
aaa-server my_authent_grp p aaa-server my_authent_grp p reactivation-mode depletion max-failed-attempts 3 aaa-server my_author_grp pr aaa-server my_author_grp pr reactivation-mode depletion max-failed-attempts 3	rotocol kerberos rotocol kerberos deadtime 10 otocol Idap otocol Idap deadtime 10		<u></u>
1	Send Can	ncel	¥ 2

I gruppi di server appena creati devono ora essere popolati con server di autenticazione e autorizzazione.

6. Scegliere Configurazione > Proprietà > Impostazione AAA > Server AAA, quindi fare clic su Aggiungi.



7. Configurare un server di autenticazione. Al termine, fare clic su

				×
Server Group:		my_authent_grp		•
Interface Name:		inside		•
Server IP Address:		172.22.1.100		
Timeout:		10	seconds	
–Kerberos Parame	ters ———			
Server Port:	88			
Server Port: Retry Interval:	88 10 seconds	s		•
Server Port: Retry Interval: Kerberos Realm:	88 10 seconds REALM.CIS	s SCO.COM		•
Server Port: Retry Interval: Kerberos Realm:	88 10 seconds REALM.CIS	s SCO.COM		•
Server Port: Retry Interval: Kerberos Realm:	88 10 seconds REALM.CIS	s SCO.COM		•
Server Port: Retry Interval: Kerberos Realm:	88 10 seconds REALM.CIS	s SCO.COM		•
Server Port: Retry Interval: Kerberos Realm:	88 10 seconds REALM.CIS	s 3CO.COM		
Server Port: Retry Interval: Kerberos Realm: OK	88 10 seconds REALM.CIS	s 3CO.COM	Help	

server: scegliere il gruppo di server di autenticazione configurato nel passaggio 2.Nome interfaccia (Interface Name) - Consente di scegliere l'interfaccia su cui risiede il server.Indirizzo IP server: specificare l'indirizzo IP del server di autenticazione.Timeout: specificare il tempo massimo, in secondi, di attesa per una risposta dal server.Parametri Kerberos:Porta server—88 è la porta standard per Kerberos.Intervallo tentativi (Retry Interval) - Consente di scegliere l'intervallo dei tentativi desiderato.Realm Kerberos: immettere il nome dell'area di autenticazione Kerberos. Si tratta spesso del nome di dominio di Windows in lettere maiuscole.

8. Configurare un server di autorizzazione. Al termine, fare clic su

Server Group: my_author_grp Interface Name: inside Server IP Address: 172.22.1.101 Timeout: 10 seconds Server Port: 389 Base DN: 0u=cisco Scope: One level beneath the Base DN Naming Attribute(s): uid Login DN:	Add AAA Server	×
Interface Name: inside Server IP Address: 172.22.1.101 Timeout: 10 seconds LDAP Parameters Server Port: 389 Base DN: 0u=cisco Scope: One level beneath the Base DN • Naming Attribute(s): Uid Login DN: Uid Login Password: Confirm Login Password: UK Cancel Help	Server Group:	my_author_grp
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: OK Cancel Help	Interface Name:	inside 💌
Timeout: 10 seconds LDAP Parameters 389 Base DN: 0u=cisco Scope: One level beneath the Base DN Naming Attribute(s): uid Login DN:	Server IP Address:	172.22.1.101
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: OK Cancel Help	Timeout:	10 seconds
Server Port: 389 Base DN: ou=cisco Scope: One level beneath the Base DN Naming Attribute(s): uid Login DN:	LDAP Parameters	
Base DN: Ou=cisco Scope: One level beneath the Base DN Naming Attribute(s): uid Login DN:	Server Port:	389
Scope: One level beneath the Base DN Naming Attribute(s): uid Login DN:	Base DN:	ou=cisco
Naming Attribute(s): uid Login DN: Login Password: Confirm Login Password: Help	Scope:	One level beneath the Base DN
Login DN: Login Password: Confirm Login Password: OK Cancel Help	Naming Attribute(s):	uid
Login Password: Confirm Login Password: OK Cancel Help	Login DN:	
Confirm Login Password:	Login Password:	
OK Cancel Help	Confirm Login Password:	
OK Cancel Help		
OK Cancel Help		
<i>r</i> \\	ок	Cancel Help
a continue il annuano all'a su contantanza di una su di contanza d		
	ndirizzo IP server: specificare are il tempo massimo, in secu	e l'indirizzo IP del server di autorizzazione. Time ondi, di attesa per una risposta dal server Parar
ndirizzo IP server: specificare l'indirizzo IP del server di autorizzazione. Time are il tempo massimo, in secondi, di attesa per una risposta dal server Paran		20 à la porte di default por L DAD DN di base : im

una richiesta di autorizzazione. **Ambito**: scegliere l'estensione in base alla quale il server deve eseguire la ricerca nella gerarchia LDAP dopo aver ricevuto una richiesta di autorizzazione. **Attributi di denominazione**: immettere gli attributi Nome distinto relativo in base ai quali le voci sul server LDAP sono definite in modo univoco. Gli attributi di denominazione comuni sono il nome comune (cn) e l'ID utente (uid). **DN accesso**: alcuni server LDAP, incluso il server Microsoft Active Directory, richiedono al dispositivo di stabilire un handshake tramite binding autenticato prima di accettare richieste per altre operazioni

LDAP. Il campo DN di accesso definisce le caratteristiche di autenticazione del dispositivo, che devono corrispondere a quelle di un utente con privilegi amministrativi. Ad esempio, cn=administrator. Per l'accesso anonimo, lasciare vuoto questo campo.**Password di login**: immettere la password per il DN di login.**Conferma password di accesso**: conferma la password per il DN di accesso.

- 9. Fare clic su **Apply** (Applica) per inviare le modifiche al dispositivo dopo l'aggiunta di tutti i server di autenticazione e autorizzazione.Se è stato configurato per tale operazione, PIX visualizza ora in anteprima i comandi aggiunti alla configurazione in esecuzione.
- 10. Per inviare i comandi al dispositivo, fare clic su Send.

Configurare un gruppo di tunnel VPN per l'autenticazione e l'autorizzazione

Completare questa procedura per aggiungere i gruppi di server appena configurati a un gruppo di tunnel VPN.

 Scegliere Configurazione > VPN > Gruppo di tunnel e fare clic su Aggiungi per creare un nuovo gruppo di tunnel oppure su Modifica per modificare un gruppo esistente.



2. Nella scheda Generale della finestra visualizzata, selezionare i gruppi di server configurati in precedenza.

🞼 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. *Facoltativo:* Configurare i parametri rimanenti nelle altre schede se si aggiunge un nuovo gruppo di tunnel.
- 4. Al termine, fare clic su OK.
- 5. Fare clic su **Apply** (Applica) per inviare le modifiche al dispositivo dopo aver completato la configurazione del gruppo di tunnel.Se è stato configurato per tale operazione, PIX visualizza ora in anteprima i comandi aggiunti alla configurazione in esecuzione.
- 6. Per inviare i comandi al dispositivo, fare clic su Send.

Configurazione dell'autenticazione e dell'autorizzazione per gli utenti VPN tramite CLI

Questa è la configurazione CLI equivalente per i gruppi di server di autenticazione e autorizzazione per gli utenti VPN.

Configurazione CLI di Security Appliance

```
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
1
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.
```

Verifica

Completare questa procedura per verificare l'autenticazione dell'utente tra il server PIX/ASA e il server AAA:

 Scegliere Configurazione > Proprietà > Impostazione AAA > Server AAA, quindi selezionare il gruppo di server (my_authent_grp). Quindi fare clic su Test per convalidare le credenziali dell'utente.

👔 Cisco ASDM 5	.0 for PIX - 10.89.129.147					_10
File Rules St	arch Options Tools Wizar	ds Help				
💰 Home	Configuration Monitoring	Back Forv	vard Search	Refresh Save	? Help	Cisco Syste
Features	Configuration > Features > P	roperties > AAA B	etup > AAA Server	5		
Interfaces		AAA Servers - Add and corr go to the AAA	Igure AAA servers	for existing AAA serve	r groups. To configure s	erver groups
Security Policy	🕀 🐻 Advanced	Serve	r Group (Protocol)	Interface	Server IP Address	Timeout 14d
	Anti-Spoofing	(my_auti	nent_grp	inside	172.22.1.100	
Routing Routing Building Blocks	Auto Update DHCP Services - P DHCP Server - DHCP Relay - DNS Client - Fallover					Tesia

2. Fornire il nome utente e la password (ad esempio, nome utente: test e password: test) e fare clic su **OK** per

•	🔂 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
	C Authorization	O Authentication
	Username:	test
	Password:	***
convalidare.	ок	Cancel

3. L'autenticazione ha esito



Risoluzione dei problemi

- 1. Una causa frequente degli errori di autenticazione è lo sfasamento dell'orologio. Accertarsi quindi che gli orologi del PIX o dell'ASA e del server di autenticazione siano sincronizzati.Quando l'autenticazione non riesce a causa dell'inclinazione dell'orologio, è possibile ricevere questo messaggio di errore: ERRORE: Autenticazione rifiutata: Inclinazione dell'orologio maggiore di 300 secondi.. Viene inoltre visualizzato il seguente messaggio di registro:%PIX|ASA-3-113020: Errore Kerberos: Sfasamento dell'orologio con indirizzo_ip del server maggiore di 300 secondi ip_address: l'indirizzo IP del server Kerberos dell'orologio di un utente IPSec o WebVPN tramite un server Kerberos ha esito negativo a causa di una differenza di tempo tra gli orologi dell'accessorio di protezione e del server di più di cinque minuti (300 secondi). In questo caso, il tentativo di connessione viene rifiutato.Per risolvere il problema, sincronizzare gli orologi dell'accessorio di protezione e del server Kerberos.
- 2. È necessario disabilitare la preautenticazione in Active Directory (AD) oppure potrebbe verificarsi un errore di autenticazione utente.
- 3. Gli utenti del client VPN non sono in grado di eseguire l'autenticazione sul server certificati Microsoft. Viene visualizzato questo messaggio di errore:"Errore durante l'elaborazione del payload" (Errore 14) Per risolvere il problema, deselezionare la casella di controllo **Non richiedere preautenticazione kerberosa** nel server di autenticazione.

Informazioni correlate

- <u>Configurazione dei server AAA e del database locale</u>
- Cisco ASA serie 5500 Adaptive Security Appliance Supporto dei prodotti
- Software Cisco PIX Firewall
- Riferimenti per i comandi di Cisco Secure PIX Firewall
- Avvisi sui prodotti per la sicurezza (inclusi PIX)
- RFC (Requests for Comments)
- Documentazione e supporto tecnico Cisco Systems