PIX/ASA: Konfigurationsbeispiel für die Kerberos-Authentifizierung und LDAP-Autorisierungsserver-Gruppen für VPN-Client-Benutzer über ASDM/CLI

Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Zugehörige Produkte Konventionen Hintergrundinformationen Konfigurieren der Authentifizierung und Autorisierung für VPN-Benutzer mithilfe von ASDM Authentifizierungs- und Autorisierungsserver konfigurieren Konfigurieren einer VPN-Tunnel-Gruppe für Authentifizierung und Autorisierung Konfigurieren der Authentifizierung und Autorisierung für VPN-Benutzer mithilfe der CLI Überprüfen Fehlerbehebung Zugehörige Informationen

Einführung

In diesem Dokument wird beschrieben, wie Sie mit dem Cisco Adaptive Security Device Manager (ASDM) die Kerberos-Authentifizierung und LDAP-Autorisierungsserver-Gruppen auf den Sicherheitslösungen der Serie Cisco PIX 500 konfigurieren. In diesem Beispiel werden die Servergruppen von der Richtlinie einer VPN-Tunnelgruppe verwendet, um eingehende Benutzer zu authentifizieren und zu autorisieren.

Voraussetzungen

<u>Anforderungen</u>

In diesem Dokument wird davon ausgegangen, dass das PIX vollständig betriebsbereit ist und so konfiguriert ist, dass der ASDM Konfigurationsänderungen vornehmen kann.

Hinweis: Informationen zur Konfiguration des PIX durch den ASDM finden Sie unter <u>Zulassen von</u> <u>HTTPS-Zugriff für ASDM</u>.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco PIX Security Appliance Software Version 7.x oder höher
- Cisco ASDM Version 5.x und höher

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Zugehörige Produkte

Diese Konfiguration kann auch mit der Cisco Adaptive Security Appliance (ASA) Version 7.x verwendet werden.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den <u>Cisco Technical Tips</u> <u>Conventions</u> (Technische Tipps zu Konventionen von Cisco).

Hintergrundinformationen

Nicht alle möglichen Authentifizierungs- und Autorisierungsmethoden, die in der PIX/ASA 7.x-Software verfügbar sind, werden unterstützt, wenn Sie mit VPN-Benutzern umgehen. In dieser Tabelle sind die für VPN-Benutzer verfügbaren Methoden aufgeführt:

	Lok al	RADI US	TACAC S+	SD I	ΝΤ	Kerber os	LD AP
Authentifizie rung	Ja	Ja	Ja	Ja	Ja	Ja	Nei n
Autorisierun g	Ja	Ja	Nein	Ne in	Ne in	Nein	Ja

Hinweis: Kerberos wird für die Authentifizierung und LDAP für die Autorisierung von VPN-Benutzern in diesem Beispiel verwendet.

Konfigurieren der Authentifizierung und Autorisierung für VPN-Benutzer mithilfe von ASDM

Authentifizierungs- und Autorisierungsserver konfigurieren

Führen Sie diese Schritte aus, um die Authentifizierungs- und Autorisierungsserver-Gruppen für VPN-Benutzer über ASDM zu konfigurieren.

1. Wählen Sie Konfiguration > Eigenschaften > AAA-Setup > AAA-Servergruppen aus, und

klicken Sie auf Hinzufügen



 Definieren Sie einen Namen f
ür die neue Authentifizierungsservergruppe, und w
ählen Sie ein Protokoll aus.Die Option Accounting Mode ist nur f
ür RADIUS und TACACS+ verf
ügbar. Klicken Sie abschlie
ßend auf



3. Wiederholen Sie die Schritte 1 und 2, um eine neue Autorisierungsserver-Gruppe zu

	🔂 Add AAA Server Gro	pup		×
	Configure AAA server applicable for RADIUS	group. The Accounting 3 and TACACS+ protoc) 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		
erstellen.	ОК	Cancel	Help	

4. Klicken Sie auf **Apply**, um die Änderungen an das Gerät zu senden.



Wenn Sie dies konfiguriert haben, zeigt das Gerät jetzt die Befehle vorab an, die der aktuellen Konfiguration hinzugefügt werden.

5. Klicken Sie auf **Senden**, um die Befehle an das Gerät zu senden.

review CLI Commands	
The following CLI commands are generated based on the changes you made in ASDM. To send the commands to the PIX, click Send. To not send the commands and continue making changes in ASDM, click Cancel.	
aaa-server my_authent_grp protocol kerberos aaa-server my_authent_grp protocol kerberos reactivation-mode depletion deadtime 10 max-failed-attempts 3 aaa-server my_author_grp protocol Idap aaa-server my_author_grp protocol Idap reactivation-mode depletion deadtime 10 max-failed-attempts 3	4
	ہ ا
Send Cancel	-

Die neu erstellten Servergruppen müssen nun mit Authentifizierungs- und Autorisierungsservern gefüllt werden.

6. Wählen Sie Konfiguration > Eigenschaften > AAA-Setup > AAA-Server aus, und klicken Sie auf

Hinzufügen.



7. Konfigurieren Sie einen Authentifizierungsserver. Klicken Sie abschließend auf

Add AAA Server						×
Server Group:		my_auth	ent_grp		•	
Interface Name:		inside			•	
Server IP Address:		172.22.1	.100			
Timeout:		10		seconds		
-Kerberos Parame	ters					1
	00					
Server Port:	88					
Server Port: Retry Interval:	88 10 second	S			•	
Server Port: Retry Interval: Kerberos Realm:	88 10 second REALM.CIS	s 3CO.COM			•	
Server Port: Retry Interval: Kerberos Realm:	88 10 second REALM.CIS	s BCO.COM			•	
Server Port: Retry Interval: Kerberos Realm:	88 10 second REALM.CIS	s SCO.COM			•	
Server Port: Retry Interval: Kerberos Realm:	88 10 second REALM.CIS	s SCO.COM			•	
Server Port: Retry Interval: Kerberos Realm:	88 10 second REALM.CIS	s BCO.COM			•	
Server Port: Retry Interval: Kerberos Realm:	88 10 second REALM.CIS	s BCO.COM				

uppe: Wählen Sie die in Schritt 2 konfigurierte Authentifizierungsservergruppe aus.Interface Name (Schnittstellenname): Wählen Sie die Schnittstelle aus, auf der sich der Server befindet.Server IP Address (Server-IP-Adresse): Geben Sie die IP-Adresse des Authentifizierungsservers an.Timeout (Zeitüberschreitung): Geben Sie die maximale Zeit (in Sekunden) an, um auf eine Antwort vom Server zu warten.Kerberos-Parameter:Server Port -88 ist der Standardport für Kerberos.Retry Interval (Wiederholintervall wiederholen): Wählen Sie das gewünschte Wiederholungsintervall aus.Kerberos Realm: Geben Sie den Namen Ihres Kerberos-Bereichs ein. Dies ist häufig der Windows-Domänenname in Großbuchstaben.

8. Konfigurieren Sie einen Autorisierungsserver. Klicken Sie abschließend auf

Add AAA Server	×
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
Confirm Login Password:	Cancel Help

Name (Schnittstellenname): Wählen Sie die Schnittstelle aus, auf der sich der Server befindet.Server IP Address (Server-IP-Adresse): Geben Sie die IP-Adresse des Autorisierungsservers an.Timeout (Zeitüberschreitung): Geben Sie die maximale Zeit (in Sekunden) an, um auf eine Antwort vom Server zu warten.LDAP-Parameter:Server Port -389 ist der Standard-Port für LDAP.Basis-DN - Geben Sie den Speicherort in der LDAP-Hierarchie ein, an dem der Server nach Erhalt einer Autorisierungsanfrage suchen soll.Scope (Umfang): Wählen Sie aus, in welchem Umfang der Server nach Erhalt einer Autorisierungsanfrage die LDAP-Hierarchie durchsuchen soll.Naming Attribute(s) - Geben Sie die Attribute für den relativen Distinguished Name ein, durch die Einträge auf dem LDAP-Server eindeutig definiert sind. Allgemeine Namensattribute sind Common Name (cn) und User ID (uid).Anmelde-DN - Einige LDAP-Server, einschließlich des Microsoft Active Directory-Servers, erfordern, dass das Gerät einen Handshake über authentifizierte Bindung erstellt, bevor Anforderungen für andere LDAP-Operationen akzeptiert werden. Das Feld Login DN definiert die Authentifizierungsmerkmale des Geräts, die denen eines Benutzers mit Administratorberechtigungen entsprechen sollten. Zum Beispiel cn=administrator. Lassen Sie dieses Feld für den anonymen Zugriff leer.**Login Password** (Anmeldekennwort): Geben Sie das Kennwort für die Anmelde-DN ein.**Anmeldungskennwort bestätigen** - Bestätigen Sie das Kennwort für die Anmelde-DN.

- 9. Klicken Sie auf Apply, um die Änderungen nach Hinzufügen aller Authentifizierungs- und Autorisierungsserver an das Gerät zu senden. Wenn Sie dies konfiguriert haben, zeigt das PIX jetzt die Befehle an, die der aktuellen Konfiguration hinzugefügt werden.
- 10. Klicken Sie auf Senden, um die Befehle an das Gerät zu senden.

Konfigurieren einer VPN-Tunnel-Gruppe für Authentifizierung und Autorisierung

Gehen Sie wie folgt vor, um die soeben konfigurierten Servergruppen zu einer VPN-Tunnelgruppe hinzuzufügen.

 Wählen Sie Configuration > VPN > Tunnel Group, und klicken Sie auf Add, um eine neue Tunnelgruppe zu erstellen, oder Edit, um eine vorhandene Gruppe zu ändern.



 Wählen Sie auf der Registerkarte Allgemein des sich öffnenden Fensters die zuvor konfigurierten Servergruppen aus.

🚰 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. *Optional:* Konfigurieren Sie die verbleibenden Parameter auf den anderen Registerkarten, wenn Sie eine neue Tunnelgruppe hinzufügen.
- 4. Klicken Sie abschließend auf OK.
- 5. Klicken Sie auf **Apply**, um die Änderungen nach Abschluss der Tunnelgruppenkonfiguration an das Gerät zu senden.Wenn Sie dies konfiguriert haben, zeigt das PIX jetzt die Befehle an, die der aktuellen Konfiguration hinzugefügt werden.
- 6. Klicken Sie auf Senden, um die Befehle an das Gerät zu senden.

Konfigurieren der Authentifizierung und Autorisierung für VPN-Benutzer mithilfe der CLI

Dies ist die entsprechende CLI-Konfiguration für die Authentifizierungs- und Autorisierungsservergruppen für VPN-Benutzer.

CLI-Konfiguration der 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
!
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.
```

<u>Überprüfen</u>

Gehen Sie wie folgt vor, um die Benutzerauthentifizierung zwischen dem PIX/ASA- und dem AAA-Server zu überprüfen:

 Wählen Sie Configuration > Properties > AAA Setup > AAA Servers, und wählen Sie die Servergruppe (my_authent_grp) aus. Klicken Sie anschließend auf Test, um die Benutzeranmeldeinformationen zu validieren.

📬 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 図 前 氷	54 18 16 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	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 14d
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 P DHCP Services					10012
Routing	- PDHCP Sarver - PDHCP Relay - ■DNS Client					\smile
Building Blocks	Failover					

2. Geben Sie Benutzername und Kennwort ein (z. B. Benutzername: Test und Kennwort: Test), und klicken Sie auf **OK**, um zu

	💼 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:	***
validieren.	ок	Cancel

3. Sie sehen, dass die Authentifizierung erfolgreich



Fehlerbehebung

- Eine häufige Ursache für Authentifizierungsfehler ist die Zeitdifferenz. Stellen Sie sicher, dass die Uhren auf dem PIX oder ASA und Ihr Authentifizierungsserver synchronisiert sind.Wenn die Authentifizierung aufgrund von "Clock Skew" fehlschlägt, können Sie die folgende Fehlermeldung erhalten: :- FEHLER: Authentifizierung abgelehnt: Die Zeitdifferenz beträgt mehr als 300 Sekunden.. Diese Protokollmeldung wird ebenfalls angezeigt:%PIX|ASA-3-113020: Kerberos-Fehler: Zeitdifferenz mit Server ip_address größer als 300 Sekunden ip_address: Die IP-Adresse des Kerberos-Servers.Diese Meldung wird angezeigt, wenn die Authentifizierung für einen IPSec- oder WebVPN-Benutzer über einen Kerberos-Server fehlschlägt, da die Uhren auf der Sicherheits-Appliance und dem Server mehr als fünf Minuten (300 Sekunden) voneinander entfernt sind. In diesem Fall wird der Verbindungsversuch zurückgewiesen.Um dieses Problem zu beheben, synchronisieren Sie die Uhren auf der Sicherheits-Appliance und dem Kerberos-Server.
- 2. Die Vorauthentifizierung im Active Directory (AD) muss deaktiviert werden, oder sie kann zu Fehlern bei der Benutzerauthentifizierung führen.
- 3. VPN-Client-Benutzer können sich nicht anhand des Microsoft-Zertifikatsservers authentifizieren. Diese Fehlermeldung wird angezeigt: "Error Processing Payload" (Fehler bei der Verarbeitung der Payload) (Fehler 14) Um dieses Problem zu beheben, deaktivieren Sie das Kontrollkästchen keine Kerberose-Vorauthentifizierung auf dem Authentifizierungsserver.

Zugehörige Informationen

- Konfigurieren von AAA-Servern und der lokalen Datenbank
- Produkt-Support für Cisco Adaptive Security Appliances der Serie ASA 5500
- <u>Cisco PIX Firewall-Software</u>
- <u>Cisco Secure PIX Firewall Befehlsreferenzen</u>
- Problemhinweise zu Sicherheitsprodukten (einschließlich PIX)
- Anforderungen für Kommentare (RFCs)
- <u>Technischer Support und Dokumentation Cisco Systems</u>