Authentifizierungsproxy implementieren

Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Konventionen Implementieren des Authentifizierungsproxys Serverprofile Cisco Secure UNIX (TACACS+) Cisco Secure Windows (TACACS+) Was der Benutzer sieht Zugehörige Informationen

Einführung

Der Authentifizierungsproxy (auth-proxy), verfügbar in der Cisco IOS® Software Firewall Version 12.0.5.T und höher, wird zur Authentifizierung ein- und ausgehender Benutzer oder beides verwendet. Diese Benutzer werden normalerweise durch eine Zugriffsliste blockiert. Mit auth-proxy rufen die Benutzer jedoch einen Browser auf, um die Firewall zu durchlaufen und sich auf einem TACACS+- oder RADIUS-Server zu authentifizieren. Der Server übergibt zusätzliche Zugriffslisteneinträge bis zum Router, damit die Benutzer nach der Authentifizierung fortfahren können.

Dieses Dokument enthält allgemeine Tipps für den Benutzer zur Implementierung von auth-Proxy, enthält einige Cisco Secure Server-Profile für den Authentifizierungsproxy und beschreibt, was der Benutzer sieht, wenn auth-proxy verwendet wird.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips

Implementieren des Authentifizierungsproxys

Gehen Sie wie folgt vor:

- 1. Stellen Sie sicher, dass der Datenverkehr ordnungsgemäß durch die Firewall fließt, bevor Sie den auth-Proxy konfigurieren.
- 2. Um während des Testens eine minimale Unterbrechung des Netzwerks zu ermöglichen, ändern Sie die vorhandene Zugriffsliste so, dass der Zugriff auf einen Testclient verweigert wird.
- 3. Stellen Sie sicher, dass der eine Test-Client die Firewall nicht durchlaufen kann und dass die anderen Hosts durchkommen können.
- 4. Aktivieren Sie das Debuggen mit **exec-timeout 0 0** unter dem Konsolenport oder den Virtual Type Terminals (VTYs), während Sie die **auth-Proxy-**Befehle und den Test hinzufügen.

Serverprofile

Die Tests wurden mit Cisco Secure UNIX und Windows durchgeführt. Wenn RADIUS verwendet wird, muss der RADIUS-Server anbieterspezifische Attribute unterstützen (Attribut 26). Hier einige Beispiele für Server:

Cisco Secure UNIX (TACACS+)

```
# ./ViewProfile -p 9900 -u proxyonly
User Profile Information
user = proxyonly{
profile_id = 57
set server current-failed-logins = 1
profile_cycle = 2
password = clear "******"
service=auth-proxy {
  set priv-lvl=15
  set proxyacl#1="permit icmp any any"
  set proxyacl#2="permit tcp any any"
  set proxyacl#3="permit udp any any"
}
```

Cisco Secure Windows (TACACS+)

Befolgen Sie dieses Verfahren.

- 1. Geben Sie den Benutzernamen und das Kennwort ein (Cisco Secure oder Windows-Datenbank).
- 2. Wählen Sie als Schnittstellenkonfiguration TACACS+ aus.
- Wählen Sie unter Neue Dienste die Option Gruppe aus, und geben Sie auth-proxy in die Spalte Service ein. Lassen Sie die Spalte Protokoll leer.

Escosecure Austion windows sould in the Worksold Internet Explorer provided by Lisco IT Packaged It 5.5 skt						
4- Dack +	101 3	Search (affevories Stistory De Of	w • • 9		
ddress 2 http:///172.18.1	24.145118	57)index2.hi			+ c≫Ga Linka '	
Congle +	0000000000	- 6:	arch Web - @charach this - @charach	de e 🎦 📭 💌 🌶 recente 👘	요즘 같은 것은 이에서 이 것을 것을 가지 못했다. 것이 같아요.	
Cinco Searems .	atorfac	o Conf	inuration		×	
dbudh.		JE 00111	iyuraavn	2		
E NUMBER	dit				-	
Eatup			TACACS+ (Cisco	a:	TACACS+ (Cisco)	
	TACACS+ Services			43 	Advanced Configuration Options	
Configuration				2	TACACS+ (Cisco)	
Configuration						
Centigeration		R	PPP IP		Calast the sheal has far sitter Then added	
OB Administration			PPP IPX		Group for each TACACS+ service that you want	
Control		Ξ.	PPP Multilink		to appear as a configurable option in the User	
Batabase			PPP Apple Talk		Setup and/or Group Setup window, accordingly.	
Reports and	E		PPP VPDN		For correct operation, each protocol/service must	
1 Activity	E .	Π	PPP LCP		be supported by the NAS. When you have	
Deceneertation			ARAP		finished selecting options, click Submit.	
	R	R	Shell (exec)	10	It is unlikely that you will use every service and	
	E.	Ē.	SLIP		protocol available for TACACS+. Displaying	
	New Seminer				each would make setting up a user or group	
Î	THEM D	service	Semire 1	Protocol	enables you to customize the services and	
	-	æ	autorine .	(100001	protocols that are displayed.	
		2	eon-proxy			
	5	-			This list has two sections:	
i.					TACACS+ Services. This section includes the most	
-			Submit Carcal	<u>.</u>	commonly used services and protocols for	
			Containe Solicer		TACACS+ 2	
			100		internet in the second s	

- 4. Erweitert Fenster für jeden Service anzeigen benutzerdefinierte Attribute.
- 5. Aktivieren Sie unter Gruppeneinstellungen die Option **auth-proxy**, und geben Sie diese Informationen im Fenster ein:

```
priv-lvl=15
proxyacl#1=permit icmp any any
proxyacl#2=permit tcp any any
proxyacl#3=permit udp any any
```

Cisco Secure UNIX (RADIUS)

```
# ./ViewProfile -p 9900 -u proxy
User Profile Information
user = proxy{
profile_id = 58
profile_cycle = 1
radius=Cisco {
check_items= {
2="proxy"
}
reply_attributes= {
9,1="auth-proxy:priv-lvl=15"
9,1="auth-proxy:proxyacl#1=permit icmp any any"
9,1="auth-proxy:proxyacl#2=permit tcp any any"
9,1="auth-proxy:proxyacl#3=permit udp any any"
}
}
```

Cisco Secure Windows (RADIUS)

Befolgen Sie dieses Verfahren.

- 1. Öffnen Sie die Netzwerkkonfiguration. NAS sollte Cisco RADIUS sein.
- 2. Wenn die Schnittstellenkonfiguration RADIUS verfügbar ist, aktivieren Sie die VSA-Kontrollkästchen.
- 3. Geben Sie unter User Settings (Benutzereinstellungen) den Benutzernamen/das Kennwort ein.
- 4. Wählen Sie unter "Gruppeneinstellungen" die Option für **[009/001] cisco-av-pair aus**. Geben Sie in das Textfeld unter der Auswahl Folgendes ein:

```
auth-proxy:priv-lvl=15
auth-proxy:proxyacl#1=permit icmp any any
auth-proxy:proxyacl#2=permit tcp any any
auth-proxy:proxyacl#3=permit udp any any
```

Dieses Fenster ist ein Beispiel für diesen



Was der Benutzer sieht

Der Benutzer versucht, etwas auf der anderen Seite der Firewall zu durchsuchen.

Es wird ein Fenster mit dieser Meldung angezeigt:

Cisco <hostname> Firewall Authentication Proxy Username: Password:

Wenn Benutzername und Kennwort gut sind, sieht der Benutzer Folgendes:

Cisco Systems Authentication Successful! Wenn die Authentifizierung fehlschlägt, lautet die Meldung:

Cisco Systems Authentication Failed!

Zugehörige Informationen

- Support-Seite für IOS-Firewall
- <u>Technischer Support und Dokumentation Cisco Systems</u>