# Implementazione del proxy di autenticazione

# Sommario

Introduzione Prerequisiti Requisiti Componenti usati Convenzioni Come implementare il proxy di autenticazione Profili server Cisco Secure UNIX (TACACS+) Cisco Secure Windows (TACACS+) Cosa vede l'utente Informazioni correlate

# **Introduzione**

Il proxy di autenticazione (auth-proxy), disponibile nella versione 12.0.5.T di Cisco IOS® Software Firewall e successive, viene utilizzato per autenticare gli utenti in entrata o in uscita o entrambi. Questi utenti sono in genere bloccati da un elenco di accesso. Tuttavia, con il proxy di autenticazione, gli utenti configurano il browser in modo che ignori il firewall e venga autenticato su un server TACACS+ o RADIUS. Il server comunica al router altre voci dell'elenco degli accessi in modo da permettere il passaggio del traffico dopo l'autenticazione.

Questo documento fornisce all'utente suggerimenti generali per l'implementazione di auth-proxy, fornisce alcuni profili di server Cisco Secure per auth proxy e descrive ciò che l'utente vede quando si usa auth-proxy.

### **Prerequisiti**

#### **Requisiti**

Nessun requisito specifico previsto per questo documento.

#### Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

#### **Convenzioni**

Per ulteriori informazioni sulle convenzioni usate, consultare il documento <u>Cisco sulle convenzioni</u> <u>nei suggerimenti tecnici</u>.

## Come implementare il proxy di autenticazione

Attenersi alla seguente procedura:

- 1. Prima di configurare il proxy di autenticazione, verificare che il traffico scorra correttamente attraverso il firewall.
- 2. Per ridurre al minimo l'interruzione della rete durante il test, modificare l'elenco degli accessi esistente in modo da negare l'accesso a un client di test.
- 3. Verificare che un client di test non possa attraversare il firewall e che gli altri host possano passare.
- 4. Attivare il debug con **exec-timeout 0 0** sulla porta della console o sui terminali virtuali (VTY), mentre si aggiungono i comandi **auth-proxy** e si esegue il test.

#### Profili server

Il test è stato eseguito con Cisco Secure UNIX e Windows. Se RADIUS è in uso, il server RADIUS deve supportare attributi specifici del fornitore (attributo 26). Di seguito sono riportati esempi specifici di 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+)
```

Attenersi alla procedura seguente.

- 1. Immettere il nome utente e la password (database Cisco Secure o Windows).
- 2. Per Interface Configuration (Configurazione interfaccia), selezionare TACACS+.
- 3. In Nuovi servizi selezionare l'opzione **Group** e digitare **auth-proxy** nella colonna Service. Lasciare vuota la colonna Protocollo.

CiscoSecure ACS for Wi	indows 21	000/NT - Mi	rosoft Internet Explorer provided by Cisco IT Packaged BE 5.5	541 LICIX
File Edit Yiev Favo	rikes Tor	ols Help		
Hoak + - O	8 00 1	Clanarch (	Jeventes Stistery 2. J W . J K	
andle .	124.14510	es/index2.h	n an an a	T (* Ga   Linka *
and due of		- 0-×		
Cisco Sestems	nterfa	ce Conf	iguration	×
albadba	Edit			El Help
Diver Setup	TACACS+ (Cisco)			TACACS+ (Cisco)     Advanced Configuration Options
Configuration				
Configuration	User	Group	,	TACACS+ (Cisco)
Leterface Cenfiguration		R	PPP IP	Select the check how for either User and/or
L + Administration	E.		PPP IPX	Group for each TACACS+ service that you want
Contriol			PPP Multilink	to appear as a configurable option in the User
External Uper Databases			PPP Apple Talk	Setup and/or Group Setup window, accordingly.
oports and	E	E	PPP VPDN	For correct operation, each protocol/service must
dias	E .		PPP LCP	be supported by the NAS. When you have
convertation		E	ARAP	inished selecting options, click Subilit.
	R	R	Shell (exec)	It is unlikely that you will use every service and
			SLIP	protocol available for TACACS+. Displaying
	New Services			each would make setting up a user or group cumbersome. To simplify setup, this section enables you to customize the services and
	-		Service Protocol	protocols that are displayed.
		1	eun-prov	
	1	-		This list has two sections:
	10			TACACS+ Services. This section includes the most
-			Submit Carriel	commonly used services and protocols for
			Sanatine Concer	TACACS+
				internet

- 4. Avanzate finestra di visualizzazione per ciascun servizio attributi personalizzati.
- 5. In Impostazioni gruppo, selezionare **auth-proxy** e immettere queste informazioni nella finestra:

```
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"
}
}
```

Attenersi alla procedura seguente.

......

- 1. Aprire Configurazione di rete. NAS deve essere Cisco RADIUS.
- 2. Se è disponibile la configurazione interfaccia RADIUS, selezionare le caselle VSA.
- 3. In Impostazioni utente, immettere nome utente/password.
- 4. In Impostazioni gruppo, selezionare l'opzione per **[009/001] cisco-av-pair**. Nella casella di testo sotto la selezione, digitare quanto segue:

```
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
```

Questa finestra è un esempio di questo

CiscoSecure ACS for	Windows 2000/HT - Microsoft Internet Explorer	
jie gol yew ryn ↓→ . → Back	- Control Cont	]- ∰- ⊉ ⊉ 👱 Ial Size Pirt Real.com Messenge
Agidents 🔄 http://127.00	31:4945/	🖻 🖗 So 🛛 Urka '
Cisco Sverems	Group Setup	X
dhuudhu	Jung Te RADIUS (Cisco IOS/Pb)	Help
User Setup		
Setup		Voice-over. (P (VoIP) Support     Default Time-of Day Access Settings
Shared Profile Comparents	Cisco IOS/PIX RADRUS Attributes	Colling Access Restrictions     May Consider a
Astwork Configuration	1009001] caso-av-pair	Inits designer     Gage Questar     Enable Options     Token Card Settings     Pornoul Aging Rules     P Assignment     Devenlendable ACLs     TACACS+ Settings     TACACS+ Settings     TACACS+ Shell Command Authorization     TACACS+ Unknown Services     ETF EADUS Authoutes
Sector Configuration	auth-proxy:priv-lvl=15 auth-proxy:proxyacl#1=permit long any any auth-proxy:proxyacl#2=permit	
Configuration	tep any any	
Centrol	[009401] cscc-k323-credit-senorast	
Del Datebarer	[ [009402] cisco-3223-credit-time	EAULUS Vender-Specific Attributes
Activity		
Documentation	D (2007103) cisco-5323-ntum-code	Group Settings To eachle administrators to tailor what authorizations are displayed for a configuration and to simplify the interface, Circo Secure ACS displays only the information for the current configuration. Specific Oroup Setup configuration options and security protocol attributes are
	1. [009104] cisco-6.523-prosp1+6	
	[1009105] care-b321-day-and-tane	A AAA client that uses the specified protocol has been could gured in the     Hatwork Configuration action. For example, PhD025 estimates actions
	Submit Submit+Restart Cencel	you have configured a AAA clear that uses RADOUS The specific service, postcools, and altributes have been adjected for display for the appropriate protocols in the Interface Configuration section
C]Dote		Venet

# Cosa vede l'utente

L'utente tenta di sfogliare qualcosa che si trova dall'altro lato del firewall.

Viene visualizzata una finestra con il seguente messaggio:

Cisco <hostname> Firewall Authentication Proxy Username: Password: Se il nome utente e la password sono validi, l'utente vedrà:

Cisco Systems Authentication Successful! Se l'autenticazione non riesce, il messaggio è:

Cisco Systems Authentication Failed!

### Informazioni correlate

- Pagina di supporto di IOS Firewall
- Documentazione e supporto tecnico Cisco Systems