Esempio di configurazione dell'autenticazione ASA cut-through e diretta

Sommario

Introduzione Prerequisiti Requisiti Componenti usati Convenzioni Cut-through Autenticazione diretta

Introduzione

In questo documento viene descritto come configurare l'autenticazione ASA cut-through e diretta.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Per la stesura del documento, è stata usata una appliance Cisco Adaptive Security Appliance (ASA).

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.

Convenzioni

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

Cut-through

L'autenticazione cut-through era stata configurata in precedenza con il comando **aaa authentication include**. A questo punto, viene usato il comando **aaa authentication match**. Il traffico che richiede l'autenticazione viene autorizzato in un elenco degli accessi a cui fa riferimento il comando **aaa authentication match**, in modo che l'host venga autenticato prima che il traffico specificato venga autorizzato tramite l'ASA. Di seguito è riportato un esempio di configurazione per l'autenticazione del traffico Web:

username cisco password cisco privilege 15 access-list authmatch permit tcp any any eq 80 aaa authentication match authmatch inside LOCAL

Questa soluzione funziona perché il protocollo HTTP è un protocollo in cui l'ASA può inserire l'autenticazione. L'ASA intercetta il traffico HTTP e lo autentica tramite autenticazione HTTP. Poiché l'autenticazione viene iniettata in linea, nel browser Web viene visualizzata una finestra di dialogo di autenticazione HTTP, come illustrato nella seguente immagine:

🖉 Navigation Canceled - Windows Internet Explorer	3
✓ ✓ http://192.168.1.1/	•
🚖 Favorites 🛛 🚔 🙋 Suggested Sites 🔻 🔊 Web Slice Gallery 👻	
🔾 Connecting 🖄 🔻 🖾 👻 Page 👻 Safety 👻 Tools 👻 🔞	,
Navigation to the webpage was canceled	_
Windows security Image: Constraint of the server 192.168.1.1 at Authentication Required requires a username and password. Image: Refresh the server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection). Image: Username is the server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection). Image: Username is the server is requesting that your username is the server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection). Image: Username is the server is requesting that your username and password is the server is requesting that your username and password is the server is requesting that your username and password is the server is requesting that your username and password is the server is requesting that your username and password is the server is requesting that your username and password is the server is requesting that your username and password is the server is requested in an insecure connection). Image: Username is the server is requested is the server	
Waiting for http://192.1	.4

Autenticazione diretta

L'autenticazione diretta era stata precedentemente configurata con i comandi aaa authentication include e virtual</protocol>. A questo punto, vengono utilizzati i comandi aaa authentication match e aaa authentication listener.

Per i protocolli che non supportano l'autenticazione nativa, ovvero i protocolli che non possono avere una richiesta di autenticazione in linea, è possibile configurare l'autenticazione ASA diretta. Per impostazione predefinita, l'appliance ASA non è in ascolto delle richieste di autenticazione. È possibile configurare un listener su una porta e un'interfaccia specifiche con il comando **aaa authentication listener**.

Di seguito è riportato un esempio di configurazione che permette il traffico TCP/3389 attraverso

l'appliance ASA dopo che l'host è stato autenticato:

username cisco password cisco privilege 15 access-list authmatch permit tcp any any eq 3389 access-list authmatch permit tcp any host 10.245.112.1 eq 5555 aaa authentication match authmatch inside LOCAL aaa authentication listener http inside port 5555

Prendere nota del numero di porta utilizzato dal listener (TCP/5555). L'output del comando **show asp table socket** mostra che l'ASA è in attesa delle richieste di connessione con questa porta all'indirizzo IP assegnato all'interfaccia (interna) specificata.

ciscoasa(config)# show asp table socket

Protocol Socket Local Address Foreign Address State
TCP 000574cf 10.245.112.1:5555 0.0.0.0:* LISTEN
ciscoasa(config)#

Dopo aver configurato l'ASA come mostrato sopra, un tentativo di connessione tramite l'ASA a un host esterno sulla porta TCP 3389 determinerà un rifiuto di connessione. L'utente deve prima eseguire l'autenticazione per consentire il traffico TCP/3389.

L'autenticazione diretta implica che l'utente debba passare direttamente all'appliance ASA. Se si sceglie http://<*asa_ip*>:<*port*>, viene restituito un errore 404 in quanto non esiste alcuna pagina Web nella directory principale del server Web dell'appliance ASA.

🏉 HTTP 404	Not Found - Windows Internet Explorer		
@ •	http://10.245.112.1:5555/	• + × P Bing	• ٩
🚖 Favorites	🚔 🙋 Suggested Sites 🔻 🙋 Web Slice Gallery 👻		
🏉 НТТР 40	4 Not Found	🟠 🔻 🗟 👻 🖃 🖶 👻 Page 👻 Safety	🕶 Tools 🕶 🔞 🕶
1	The webpage cannot be found		HTTP 404
	Most likely causes: • There might be a typing error in the address. • If you clicked on a link, it may be out of date.		
	What you can try:		
	Retype the address.		
	 Go back to the previous page. 		
	 Go to and look for the information you want. 		
	More information		
			- 100%
Done	🤤 Inter	net Protected Mode: Un	v 100% ▼

Èinvece necessario passare direttamente a

http://<asa_ip>:</istener_port>/netaccess/connstatus.html. In corrispondenza di questo URL si trova una pagina di accesso in cui è possibile fornire le credenziali di autenticazione.

🥖 Cisco Systems, Inc. Network Access - Windows Internet Explorer	
	+ م
🖕 Favorites 🛛 🚔 💋 Suggested Sites 👻 💋 Web Slice Gallery 👻	
🍘 Cisco Systems, Inc. Network Access 🋛 👘 🔻 🖾 👻 🖶 👻 Page 👻 Safety	▼ Tools ▼ 🕢 ▼
Network User Authentication Network User Authentication is <i>required</i> .	*
Log In Now You are not logged in. User IP: 10.240.253.241	
	-
Done Sone Sone Sone Sone Sone Sone Sone S	🔍 100% 🔻 🔡

🥖 Cisco Systems, Inc. Network Access - Windows Internet Explorer	
	+ م
🔶 Favorites 🛛 🚔 🔊 Suggested Sites 🔻 🔊 Web Slice Gallery 👻	
🍘 Cisco Systems, Inc. Network Access 🎒 👻 🖾 👻 Page 👻 Safety	▼ Tools ▼ 🔞 ▼
Network User Authentication	*
Authentication Required	*
	~
Enter the following information to log in to the remote network. Please wait for the operation to complete.	
Username admin	
Password •••••	
Continue Cancel	
	Ŧ
/netaccess/loginuser.html 😜 Internet Protected Mode: On 🦓 🔻	🔍 100% 🔻 🔡

🏉 Cisco Systems, Inc. Network Access - Windows Internet Explorer	
	+ م
🚖 Favorites 🛛 🚔 🔊 Suggested Sites 👻 🔊 Web Slice Gallery 👻	
🍘 🗸 🔝 🔹 🖾 🔹 Page 🛪 Safety	/ 🕶 Tools 👻 🔞 👻
Network User Authentication	*
Access Granted	*
Log Out Now You are logged in. Username: admin User IP: 10.240.253.241 Since: 09:28:45 UTC Mon Dec 12 2011 (for Hours: 0 Min: 0 Sec: 0)	
Done 🕥 Internet Protected Mode: On	🔻 🔍 100% 👻 💡

In questa configurazione, il traffico di autenticazione diretta fa parte dell'elenco degli accessi authmatch. Senza questa voce di controllo di accesso, è possibile che venga visualizzato un messaggio non previsto, ad esempio *Autenticazione utente*. *L'autenticazione utente non* è *necessaria*, quando si passa a http://<*asa_ip*>:<*listener_port*>/netaccess/connstatus.html.

🤗 Cisco Systems, Inc. Network Access - Windows Internet Explorer	
🚱 🕞 🗢 🙋 http://10.245.112.1:5555/netaccess/connstatus.html 🔻 🗟 🍫 🗙 🔑 Bing	+ م
🖕 Favorites 🛛 👍 🙋 Suggested Sites 👻 🙋 Web Slice Gallery 👻	
🍘 🗸 🔝 👻 🖾 👻 Page 🛪 Safety	🔹 Tools 👻 🔞 💌
User Authentication	*
User Authentication is not required.	
	-
Done Sinternet Protected Mode: On 🖓	🕶 🔍 100% 🔻 🖽

Dopo aver eseguito l'autenticazione, è possibile connettersi tramite l'ASA a un server esterno su TCP/3389.