Strumento WebVPN Capture su Cisco ASA serie 5500 Adaptive Security Appliance

Sommario

Introduzione

Cisco ASA serie 5500 Adaptive Security Appliance include uno strumento di acquisizione WebVPN che consente di registrare le informazioni sui siti Web che non vengono visualizzati correttamente su una connessione WebVPN. È possibile attivare lo strumento di acquisizione dall'interfaccia CLI (Command Line Interface) dell'accessorio di protezione. I dati registrati da questo strumento possono essere utili al rappresentante dell'assistenza clienti Cisco per risolvere i problemi.

Nota: l'abilitazione dello strumento di acquisizione WebVPN ha un impatto sulle prestazioni dell'appliance di sicurezza. Assicurarsi di disattivare lo strumento di acquisizione dopo aver generato i file di output.

Prerequisiti

Requisiti

Prima di provare la configurazione, verificare che sia soddisfatto il seguente requisito:

- Per configurare Cisco ASA serie 5500 Adaptive Security Appliance, usare l'interfaccia della riga di comando (CLI).

Componenti usati

Per la stesura del documento, è stato usato Cisco ASA serie 5500 Adaptive Security Appliance con versione 7.0.

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 Cisco sulle convenzioni nei suggerimenti tecnici.

Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).

File di output dello strumento di acquisizione WebVPN

Quando lo strumento di acquisizione WebVPN è abilitato, lo strumento di acquisizione memorizza i dati del primo URL visitato nei seguenti file:

- original.000: contiene i dati scambiati tra l'appliance di sicurezza e il server Web.
- mangled.000: contiene i dati scambiati tra l'appliance di sicurezza e il browser.

Per ogni acquisizione successiva, lo strumento di acquisizione genera ulteriori file originali.<nnn> e gestiti.<nnn> e incrementa le estensioni dei file. Nell'esempio, l'output del comando **dir** visualizza tre set di file da tre acquisizioni di URL:

```
hostname#dir
Directory of disk0:/
2952        -rw-        10931           10:38:32 Jan 19 2005 config
6           -rw-        5124096         19:43:32 Jan 01 2003 cdisk.bin
3397        -rw-        5157            08:30:56 Feb 14 2005 ORIGINAL.000
3398        -rw-        6396            08:30:56 Feb 14 2005 MANGLED.000
3399        -rw-        4928            08:32:51 Feb 14 2005 ORIGINAL.001
3400        -rw-        6167            08:32:51 Feb 14 2005 MANGLED.001
3401        -rw-        5264            08:35:23 Feb 14 2005 ORIGINAL.002
3402        -rw-        6503            08:35:23 Feb 14 2005 MANGLED.002
hostname#
```

Attiva lo strumento di acquisizione WebVPN

Nota: il file system Flash presenta delle limitazioni quando si aprono più file per la scrittura. Lo strumento di acquisizione WebVPN può causare il danneggiamento del file system quando più file di acquisizione vengono aggiornati contemporaneamente. Se il problema persiste con lo strumento di acquisizione, contattare il Technical Assistance Center (TAC) di Cisco.

Per attivare lo strumento di acquisizione WebVPN, utilizzare il comando **debug menu webvpn 67**

in modalità di esecuzione privilegiata:

```
debug menu webvpn 67
```

Dove:

- **cmd** è 0 o 1. 0 disabilita l'acquisizione. 1 abilita l'acquisizione.
- **user** è il nome utente da associare per l'acquisizione dei dati.
- **url** è il prefisso URL da associare per l'acquisizione dei dati. Utilizzare uno dei seguenti formati di URL:Utilizzare /http per acquisire tutti i dati.Utilizzare /http/0/<server/percorso> per acquisire il traffico HTTP verso il server identificato da <server/percorso>.Utilizzare /https/0/<server/percorso> per acquisire il traffico HTTPS verso il server identificato da <server/percorso>.

Usare il comando **debug menu webvpn 67.0** per disabilitare l'acquisizione.

In questo esempio, lo strumento di acquisizione WebVPN è abilitato per acquisire il traffico HTTP per l'utente 2 che visita il sito Web wwwin.abcd.com/hr/people:

```
hostname#debug menu webvpn 67 1 user2 /http/0/wwwin.abcd.com/hr/people
Mangle Logging: ON
Name: "user2"
URL: "/http/0/wwwin.abcd.com/hr/people"
hostname#
```

In questo esempio, lo strumento di acquisizione WebVPN è disabilitato:

```
hostname#debug menu webvpn 67 0
Mangle Logging: OFF
Name: "user2"
URL: "/http/0/wwwin.abcd.com/hr/people"
hostname#
```

Individua e carica i file di output dello strumento di acquisizione WebVPN

Usare il comando **dir** per individuare i file di output dello strumento di acquisizione WebVPN. L'esempio mostra l'output del comando **dir** e include i file ORIGINAL.000 e MANGLED.000 generati:

```
hostname#dir
Directory of disk0:/
2952        -rw-        10931           10:38:32 Jan 19 2005 config
6         -rw-        5124096         19:43:32 Jan 01 2003 cdisk.bin
3397        -rw-        5157            08:30:56 Feb 14 2005 ORIGINAL.000
3398        -rw-        6396            08:30:56 Feb 14 2005 MANGLED.000
hostname#
```

Èpossibile caricare i file di output dello strumento di acquisizione WebVPN in un altro computer utilizzando il comando **copy flash**. In questo esempio, vengono caricati i file ORIGINAL.000 e

MANGLED.000:

```
hostname#copy flash:/original.000 tftp://10/86.194.191/original.000
Source filename [original.000]?
Address or name of remote host [10.86.194.191]?
Destination filename [original.000]?
!!!!!!
21601 bytes copied in 0.370 secs
hostname#copy flash:/mangled.000 tftp://10/86.194.191/mangled.000
Source filename [mangled.000]?
Address or name of remote host [10.86.194.191]?
Destination filename [mangled.000]?
!!!!!!
23526 bytes copied in 0.380 secs
hostname#
```

Nota: per evitare il possibile danneggiamento del file system, non consentire la sovrascrittura dei file originali.<nnn> e gestiti.<nnn> da acquisizioni precedenti. Quando si disattiva lo strumento di acquisizione, eliminare i vecchi file per evitare il danneggiamento del file system.

Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

Informazioni correlate

- Guide alla configurazione di Cisco ASA serie 5500 Adaptive Security Appliance
- Documentazione e supporto tecnico – Cisco Systems