Configurazione della funzione Shun di Cisco ASA per l'esenzione dell'appliance virtuale

Sommario

Introduzione

In questo documento viene descritto come configurare Cisco ASA in modo che esenti l'appliance virtuale dal componente di rilevamento delle minacce. Il componente Cisco ASA threat detection esegue l'ispezione dei pacchetti sul DNS e su altri protocolli. Il supporto Umbrella consiglia le seguenti modifiche alla configurazione ASA per evitare conflitti tra questa funzione e l'appliance virtuale:

- Esentare l'appliance virtuale dalla funzionalità di rilevamento delle minacce 'shun' come descritto in questo articolo.
- Esentare l'appliance virtuale dall'ispezione dei pacchetti DNS per consentire la crittografia DNS (DNScrypt) descritta in questo articolo: Cisco ASA Firewall blocca DNScrypt.

Funzione 'Shun' di rilevamento minacce

Quando la funzione 'Shun' è abilitata, l'ASA può bloccare completamente un indirizzo IP di origine che attiva le regole di rilevamento delle minacce. Per ulteriori informazioni, consultare l'articolo di Cisco: Funzionalità e configurazione del rilevamento delle minacce ASA.

In genere, l'appliance virtuale invia un numero molto elevato di query DNS ai resolver DNS Umbrella. Nei casi in cui si verifica un problema locale durante la connessione ai resolver (ad esempio un'interruzione temporanea della rete o una latenza), queste query possono avere esito negativo. A causa del volume di query inviate, anche una piccola percentuale di errori causa l'esclusione dell'appliance virtuale dall'appliance ASA; che determina un'interruzione completa del servizio DNS per un determinato periodo di tempo.

Esenzione dell'appliance virtuale

Nota: I comandi riportati in questo articolo sono da intendersi come guida e si consiglia di consultare un esperto Cisco prima di apportare qualsiasi modifica a un ambiente di produzione.

Via CLI:

- Per evitare che l'indirizzo IP dell'accessorio venga ignorato, eseguire questo comando: **no shun**

Tramite interfaccia ASDM:

- Scegliere il riquadro Configurazione > Firewall > Rilevamento minacce.
- Per evitare che l'indirizzo IP dell'accessorio venga ignorato, immettere un indirizzo nel campo 'Reti escluse da ignorare'. È possibile immettere più indirizzi o subnet separati da virgole.

Determinare se l'accessorio è stato "escluso"

In caso contrario, l'accessorio potrebbe sfuggire a qualsiasi evenienza e ciò potrebbe causare un'interruzione del servizio DNS.

Quando l'appliance virtuale non ha connettività esterna, la console Cisco ASA registra l'evento come segue:

4|Giu 06 2014 14:00:42|401004: Pacchetto ignorato: 192.168.1.3 ==> 208.67.222.222 sull'interfaccia interna
4|Giu 06 2014 14:00:42|401004: Pacchetto ignorato: 192.168.1.3 ==> 208.67.222.222 sull'interfaccia interna

Per visualizzare un elenco degli indirizzi IP attualmente ignorati, eseguire questo comando sull'appliance ASA: **show shun**

Per cancellare immediatamente gli indirizzi IP attualmente ignorati, eseguire questo comando sull'appliance ASA: **clear shun**

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).