&Informazioni sui messaggi ICMP Packet "unreachable - admin forced filter"

Sommario

Problema

Comprendere le informazioni sui pacchetti associate ai pacchetti ICMP (Internet Control Message Protocol) "unreachable - admin forced filter" (irraggiungibile - filtro vietato dall'amministratore).

Esempio di acquisizione di Cisco Secure Firewall Threat Defense (FTD):

<#root>

```
device#

show capture CAPO



106 packets captured

   1: 08:12:45.864243       198.51.100.205.7351 > 192.0.2.2.47668:  udp 111
   2: 08:12:46.400812       198.51.100.205.7351 > 192.0.2.2.47668:  udp 124
   3: 08:12:46.406320       192.0.2.2 > 198.51.100.205 icmp: host 192.0.2.2

unreachable - admin prohibited filter



   4: 08:12:47.936856       198.51.100.205.7351 > 192.0.2.2.47668:  udp 124
   5: 08:12:47.943936       192.0.2.2 > 198.51.100.205 icmp: host 192.0.2.2

 unreachable - admin prohibited filter



   6: 08:12:49.216739       198.51.100.205.7351 > 192.0.2.2.47668:  udp 124
   7: 08:12:49.222278       192.0.2.2 > 198.51.100.205 icmp: host 192.0.2.2

 unreachable - admin prohibited filter



   8: 08:12:50.096079       198.51.100.205.7351 > 192.0.2.2.47668:  udp 124
   9: 08:12:50.106363       192.0.2.2 > 198.51.100.205 icmp: host 192.0.2.2
```

unreachable - admin prohibited filter

Ambiente

Può essere visto in uno di questi prodotti:

- FTD
- Adaptive Security Appliance (ASA)

Risoluzione

Informazioni sui messaggi ICMP tipo 3, codice 13

I messaggi ICMP "unreachable - admin locked filter" corrispondono a ICMP tipo 3, codice 13 (destinazione irraggiungibile - comunicazione vietata a livello amministrativo). Questi messaggi indicano che il traffico è stato esplicitamente rifiutato da un criterio di sicurezza o da un elenco di controllo di accesso (ACL) anziché essere irraggiungibile a causa di problemi di connettività di rete.

Analisi delle informazioni di acquisizione dei pacchetti

Passaggio 1. Identificare l'origine dei messaggi ICMP "deny"

Esaminare l'acquisizione dei pacchetti per identificare i dispositivi che stanno generando le

risposte ICMP tipo 3, codice 13. In questo caso, i messaggi deny hanno origine da indirizzi IP specifici (192.0.2.2).

Passaggio 2. Esaminare le intestazioni dei pacchetti originali

I messaggi ICMP Deny contengono informazioni sui pacchetti originali che sono stati bloccati. Ciò include gli indirizzi IP di origine e di destinazione originali, le informazioni sul protocollo e i numeri di porta che hanno attivato il divieto amministrativo.

Passaggio 3. Correlazione dei messaggi di negazione con i modelli di traffico

Associare le risposte ICMP ai flussi di traffico specifici che vengono rifiutati. Ad esempio, il traffico UDP verso la porta 7351 è stato rifiutato dal dispositivo con indirizzo IP 192.0.2.2 nell'acquisizione CAPO.

Limitazioni all'analisi dell'acquisizione dei pacchetti

Quando si lavora con acquisizioni di pacchetti esportati con testo, l'analisi dettagliata pacchetto per pacchetto può essere limitata rispetto ai file cappuccio binari. Per un'analisi completa, i file di acquisizione pacchetti binari (formato pcap) forniscono informazioni più complete, tra cui:

- Intestazioni di pacchetto complete e informazioni sul payload
- Informazioni precise sui tempi
- Funzionalità complete di decodifica del protocollo
- Opzioni avanzate di filtro e analisi

Causa

La causa principale è in genere una delle seguenti:

- ACL configurati per impedire flussi di traffico specifici
- Regole del firewall che bloccano alcuni protocolli, porte o indirizzi IP

Nell'esempio, il messaggio è stato causato da un ACL a valle.

Contenuto correlato

- https://datatracker.ietf.org/doc/html/rfc792
- https://datatracker.ietf.org/doc/html/rfc1812
- https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/215092-analyze-firepower-firewall-captures-to-e.html

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).