Il traffico UDP attraverso l'ASA non riesce dopo che il collegamento dell'ISP primario è tornato online in una configurazione con due ISP

Sommario

Introduzione

Se un'appliance ASA (Adaptive Security Appliance) dispone di due interfacce in uscita per subnet di destinazione e il percorso preferito verso una destinazione viene rimosso dalla tabella di routing per un determinato periodo di tempo, le connessioni UDP (User Datagram Protocol) possono avere esito negativo quando il percorso preferito viene aggiunto nuovamente alla tabella di routing. Anche le connessioni TCP potrebbero essere interessate dal problema, ma poiché TCP rileva la perdita di pacchetti, queste connessioni vengono disattivate automaticamente dagli endpoint e ricompilate utilizzando le route ottimali dopo la modifica delle route.

Questo problema si può verificare anche se si usa un protocollo di routing e una modifica della topologia determina una modifica della tabella di routing sull'appliance ASA.

Operazioni preliminari

Requisiti

Per risolvere questo problema, la tabella di routing dell'ASA deve essere modificata. Ciò è comune con i collegamenti con due ISP in modo ridondante o quando l'ASA apprende le route tramite un IGP (OSPF, EIGRP, RIP).

Questo problema si verifica quando il collegamento dell'ISP primario torna online o quando il protocollo IGP interessato rileva una riconvergenza causata dalla sostituzione di una route meno preferita in uso dall'ASA con la route con metrica inferiore preferita. In questo caso, le connessioni durature, come le registrazioni SIP UDP, il GRE, ecc., avranno esito negativo una volta reinstallato il percorso principale o preferito nella tabella di routing dell'ASA.

Componenti usati

Le informazioni di questo documento si basano sulle seguenti versioni hardware e software:

- Qualsiasi appliance Cisco ASA serie 5500 Adaptive Security
- ASA versioni 8.2(5), 8.3(2)12, 8.4(1)1, 8.5(1) e successive

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Problema

Se si rimuove una voce della tabella di routing dalla tabella di routing dell'ASA e non ci sono route da un'interfaccia a una destinazione, le connessioni costruite attraverso il firewall con la destinazione esterna vengono eliminate dall'ASA. Questo si verifica in modo che le connessioni possano essere create di nuovo utilizzando un'interfaccia diversa con voci di routing per la destinazione presente.

Se tuttavia si aggiungono route più specifiche alla tabella, le connessioni non verranno aggiornate per utilizzare le nuove route più specifiche e continueranno a utilizzare l'interfaccia meno ottimale.

Ad esempio, considerare che il firewall ha due interfacce verso Internet - "esterne" e "di backup" - e che queste due route sono presenti nella configurazione dell'ASA:

```
route outside 0.0.0.0 0.0.0.0 10.1.1.1 1 track 1
route backup 0.0.0.0 0.0.0.0 172.16.1.1 254
```

Se sia l'interfaccia esterna che quella di backup sono attive, le connessioni costruite in uscita attraverso il firewall utilizzeranno l'interfaccia esterna, come ha la metrica preferita di 1. Se l'interfaccia esterna viene chiusa (o la funzione di monitoraggio SLA che sta tracciando il percorso rileva una perdita di connettività all'IP tracciato), le connessioni che usano l'interfaccia esterna verrebbero interrotte e ricostruite usando l'interfaccia di backup, poiché l'interfaccia di backup è l'unica interfaccia con un percorso verso la destinazione.

Il problema si verifica quando l'interfaccia esterna viene riattivata o il percorso tracciato diventa nuovamente il percorso preferito. La tabella di routing viene aggiornata in modo da preferire il percorso originale, ma le connessioni esistenti continuano a esistere sull'appliance ASA e attraversano l'interfaccia di backup e NON vengono eliminate né ricreate sull'interfaccia esterna con la metrica preferita. Infatti, il percorso predefinito di backup esiste ancora nella tabella di routing dell'interfaccia dell'ASA. La connessione continua a utilizzare l'interfaccia con il percorso meno preferito finché la connessione non viene eliminata; nel caso dell'UDP, tale valore potrebbe essere indefinito.

Questa situazione può causare problemi con le connessioni di lunga durata, come le registrazioni SIP esterne o altre connessioni UDP.

Soluzione

Per risolvere questo problema specifico, è stata aggiunta una nuova funzionalità all'appliance ASA

che causerà l'annullamento delle connessioni e la ricostruzione su una nuova interfaccia se alla tabella di routing viene aggiunto un percorso preferenziale alla destinazione. Per attivare la funzione (che è disabilitata per impostazione predefinita), impostare un timeout diverso da zero sul comando **timeout floating-conn**. Questo timeout (specificato in HH:MM:SS) specifica il tempo di attesa dell'ASA prima che la connessione venga interrotta quando si aggiunge un altro percorso preferenziale alla tabella di routing:

Questo è un esempio della CLI di abilitazione della funzione. Con questa CLI, se un pacchetto viene ricevuto su una connessione esistente per la quale ora esiste un percorso diverso, più preferito, verso la destinazione, la connessione verrà interrotta un minuto dopo (e ricompilata usando il nuovo percorso preferenziale):

```
ASA# config terminal
ASA(config)# timeout floating-conn 0:01:00
ASA(config)# end
ASA# show run timeout
timeout conn 1:00:00 half-closed 0:10:00 udp 0:50:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:01:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout xlate 0:01:00
timeout pat-xlate 0:00:30
timeout floating-conn 0:01:00
ASA#
```

Questa funzione viene aggiunta alla piattaforma ASA nelle versioni 8.2(5), 8.3(2)12, 8.4(1)1 e 8.5(1), tra cui le versioni più recenti del software ASA.

Se si esegue una versione del codice ASA che non implementa questa funzione, per risolvere il problema, è possibile scaricare manualmente le connessioni UDP che continuano a utilizzare la route meno preferita, anche se viene reso disponibile un percorso migliore tramite un **clear local-host** *<IP>* o **clear-conn** *<IP>* .

Nella sezione timeout della guida di riferimento per i comandi viene elencata la nuova funzionalità.

Informazioni correlate

- Documentazione e supporto tecnico – Cisco Systems