Comportamento WSA sul rilevamento dell'MTU del percorso con l'uso di WCCP

Sommario

Introduzione

Questo documento descrive un problema rilevato quando il router scarta i pacchetti quando la configurazione include il rilevamento del protocollo WCCP (Web Cache Communication Protocol) e della MTU (Maximum Transmission Unit) del percorso e fornisce una soluzione al problema.

Premesse

Pre-fase

Se esaminate separatamente, molte caratteristiche sono eccellenti per gestire un problema specifico. A volte, tuttavia, se si combinano due o tre tecniche, si ottiene un comportamento imbarazzante ed è necessario introdurre un'altra feature o soluzione alternativa per far sì che funzioni correttamente. Ad esempio, l'uso dello Spanning Tree e della convergenza Open Shortest Path First (OSPF) e Layer 2 (L2) richiede più tempo (20 s) rispetto all'OSPF (1 s se viene utilizzato l'intervallo inattivo minimo), ma la sostituzione dello Spanning Tree con Multiple Spanning-Tree (MST) e il suo corretto funzionamento.

lo stesso comportamento di interoperabilità è stato osservato tra il rilevamento WCCP e l'MTU del percorso; molti pensano che sia un problema dell'intestazione GRE (Generic Routing Encapsulation). Ma questo documento spiega la vera causa.

Modalità di funzionamento separato del rilevamento dell'MTU del percorso e del WCCP

Rilevamento MTU percorso

Ogni linea ha il proprio limite sulle dimensioni di un pacchetto. Se si invia un pacchetto più grande di quello supportato, viene scartato. Uno dei ruoli dei dispositivi L3 (router) sul percorso è quello di occuparsi e tagliare pacchetti di grandi dimensioni da una delle linee all'altra per garantire una comunicazione end-to-end trasparente per le capacità di ciascuna linea.

Tuttavia, talvolta gli host terminali sono configurati in modo tale che i relativi pacchetti non possano essere tagliati (ad esempio, file crittografati, chiamate vocali). Queste informazioni vengono comunicate tramite il bit "non frammentare" (DF, Don't Fragment) all'interno dell'intestazione IP. I router scartano pacchetti di questo tipo, ma cerca di segnalare il problema all'host finale tramite un messaggio ICMP (Internet Control Message Protocol) (tipo 3-Destination unreachable, codice 4 - frammentazione richiesta, ma bit DF impostato). In questo modo, l'host può inviare pacchetti più piccoli in futuro.

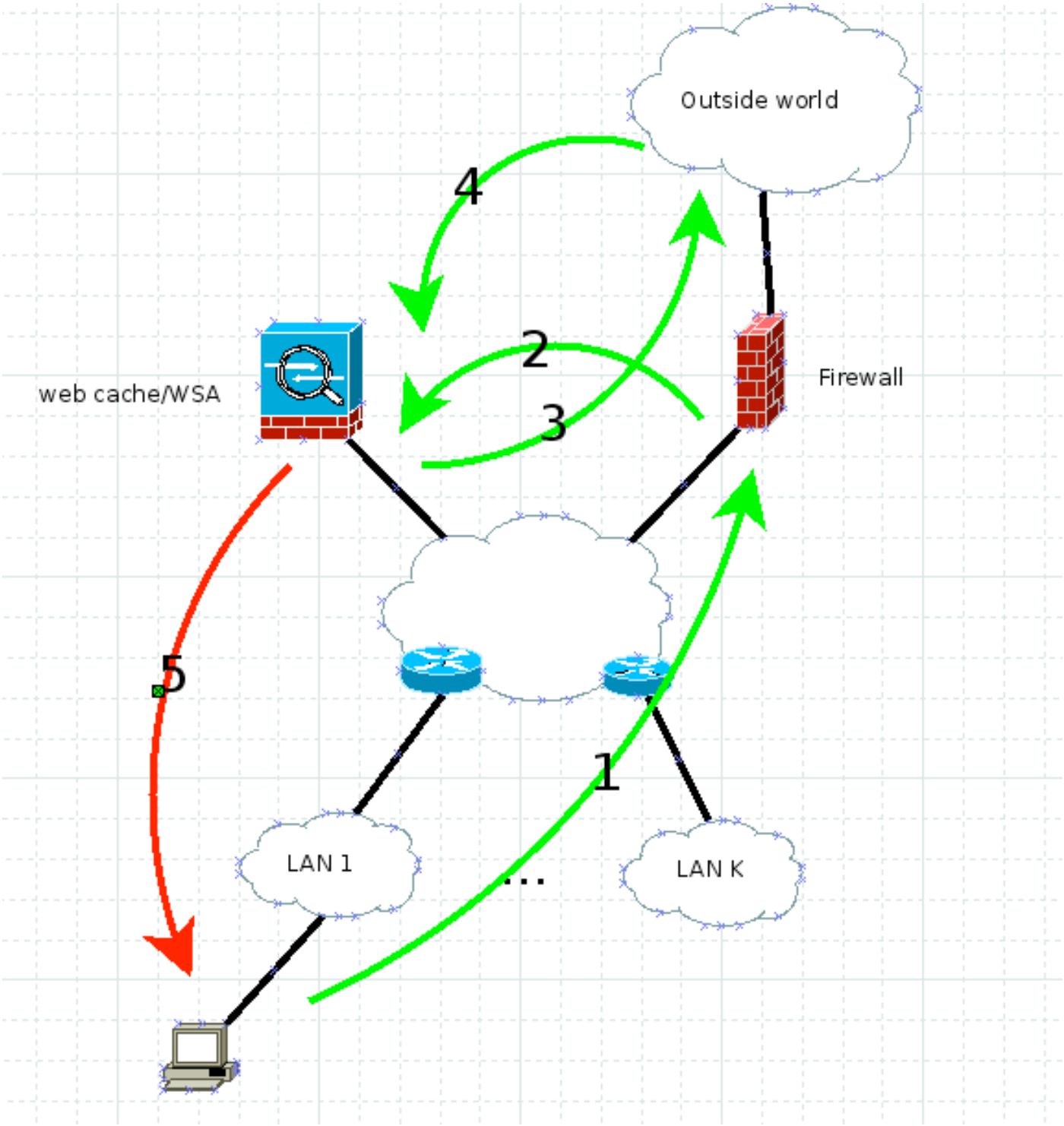
Questo è il cuore del rilevamento dell'MTU del percorso. È possibile inviare pacchetti di grandi dimensioni con il bit DF impostato per verificare se raggiungono la fine o se si riceve un rapporto ICMP come descritto in precedenza. Una volta determinate le dimensioni massime del pacchetto fattibile, utilizzarlo per ulteriori comunicazioni. Per ulteriori informazioni, fare riferimento alla RFC 1191.

Per impostazione predefinita, Web Security Appliance (WSA) utilizza il rilevamento dell'MTU del percorso. Di conseguenza, tutti i pacchetti generati hanno il bit DF impostato sulla configurazione predefinita.

WCCP

Se è necessario imporre la protezione alla rete sul traffico Web senza che altri ne siano a conoscenza, il traffico viene eseguito tramite un proxy non visibile. WCCP è il protocollo usato per comunicare tra il dispositivo che intercetta (router/firewall) e il motore/proxy della cache Web, in questo caso WSA.

Il diagramma mostra il flusso del traffico in questo scenario:



Funziona così:

1. Il client invia HTTP GET con l'origine IP, l'indirizzo IP (indirizzo IP del client) e l'indirizzo IP del server di destinazione.

2. Il firewall o il router intercetta il comando HTTP GET e lo inoltra tramite WCCP GRE o l'L2 puro alla cache Web/WSA. L'origine è ancora l'indirizzo IP del client e la destinazione è ancora l'indirizzo IP del server Web.

3. WSA esamina la richiesta e, se è legittima, la specchia verso il server Web. In questo caso, l'indirizzo IP di destinazione è l'indirizzo IP del server Web e l'indirizzo IP di origine potrebbe essere WSA o il client, a seconda che sia stato abilitato lo spoofing degli indirizzi IP dei client. Nell'esempio riportato, l'operazione non è importante in quanto il traffico di ritorno deve

in entrambi i casi raggiungere il WSA.

4. Il traffico di ritorno viene ispezionato presso il WSA.

5. Il WSA invia la risposta al client con l'indirizzo IP di origine, l'indirizzo IP del server Web ALWAYS (in modo che il client non diventi sospetto) e l'indirizzo IP del client di destinazione.

Problema

Cosa succede se uno dei router del diagramma deve frammentare il traffico? Il WSA assegna il bit DF al pacchetto numero 5, ma deve essere frammentato. Il router lo rifiuta e dice al mittente che è necessaria la frammentazione, ma il bit DF è impostato (ICMP tipo 3 codice 4). Dopo tutto, la RFC 1191 deve funzionare ora e il mittente deve ridurre le dimensioni del pacchetto.

Con WCCP, l'indirizzo IP di origine è l'indirizzo IP del server Web, quindi questo ICMP non viene mai inviato al WSA; piuttosto, cerca di andare al vero server web (ricordate, questo router in basso non è a conoscenza di WCCP). In questo modo il rilevamento WCCP e MTU del percorso a volte interrompe la progettazione della rete.

Soluzione

Esistono quattro modi per risolvere questo problema:

- Individuare l'MTU reale e usare **etherconfig** sul server WSA per abbassare la MTU dell'interfaccia. Tenere presente che l'intestazione TCP è 60, l'indirizzo IP è 20 e che quando si utilizza il protocollo ICMP, all'intestazione IP vengono aggiunti 8 byte.

- Disabilitare il rilevamento della MTU del percorso (comando **pathmtudiscovery** CLI WSA). Il valore TCP MSS di 536 potrebbe causare un problema di prestazioni.

- Modificare la rete in modo che non vi sia frammentazione L3 tra WSA e i client.

- Usare il comando **ip tcp mss-adjust 1360** (o un altro numero calcolato) su ciascun router Cisco durante il percorso sulle interfacce interessate.

Note aggiuntive

Durante l'analisi del problema, è stato scoperto che se si imposta il proxy in modo esplicito nel client per un paio di minuti e poi lo si rimuove, il problema viene risolto per le successive quattro o cinque ore. Ciò è dovuto al fatto che, in modalità esplicita, il meccanismo di rilevamento dell'MTU del percorso tra il WSA e il client funziona. Una volta rilevata l'MTU del percorso, il WSA la memorizza insieme al valore TCP MSS rilevato nella tabella interna per un riferimento. Apparentemente questa tabella viene aggiornata ogni quattro-cinque ore, il che rende la soluzione non lavorare di nuovo dopo così tanto tempo.