Guida alla progettazione di Web Security Appliance

Sommario

Introduzione

In questo documento viene descritto come progettare Cisco Web Security Appliance (WSA) e i componenti associati per prestazioni ottimali.

Premesse

Quando si progetta una soluzione per WSA, è necessario considerare attentamente non solo la configurazione dell'accessorio, ma anche i dispositivi di rete associati e le relative funzionalità. Ogni rete è una collaborazione tra più dispositivi e se uno di essi non partecipa correttamente alla rete, l'esperienza utente potrebbe non essere più disponibile.

Quando si configura il server WSA è necessario considerare due componenti principali: hardware e software. L'hardware è disponibile in due tipi diversi. La prima riguarda il tipo fisico di hardware, come i modelli delle serie S170, S380 e S680, nonché altri modelli End of Life (EoL), come i modelli delle serie S160, S360, S660, S370 e S670. L'altro tipo di hardware è virtuale, ad esempio i modelli della serie S000v, S100v e S300v. Il sistema operativo in esecuzione su questo hardware è denominato *AsyncOS for Web*, basato su FreeBSD nel suo nucleo.

WSA offre il servizio proxy e inoltre analizza, controlla e suddivide in categorie tutto il traffico (HTTP, HTTPS e FTP (File Transfer Protocol). Tutti questi protocolli vengono eseguiti su TCP e per il corretto funzionamento si basano in modo significativo sul DNS (Domain Name System). Per questi motivi, lo stato di salute della rete è fondamentale per il corretto funzionamento dell'accessorio e la sua comunicazione con varie parti della rete, sia all'interno che all'esterno del controllo aziendale.

Progettazione

Utilizzare le informazioni descritte in questa sezione per progettare il WSA e i relativi componenti per prestazioni ottimali.

Rete

Una rete rapida e priva di errori è fondamentale per il corretto funzionamento del WSA. Se la rete è instabile, l'esperienza utente potrebbe diminuire. I problemi di rete vengono in genere rilevati quando le pagine Web richiedono tempi di connessione più lunghi o non sono raggiungibili. L'inclinazione iniziale è da imputare all'accessorio, ma in genere è la rete a comportarsi in modo errato. Pertanto, è necessario prendere in considerazione e controllare attentamente per garantire che la rete offra il servizio migliore per i protocolli applicativi di alto livello come HTTP, HTTPS, FTP e DNS.

Considerazioni generali

Di seguito sono riportate alcune considerazioni generali che è possibile implementare per garantire il miglior comportamento della rete:

- Verificare che la rete di layer 2 (L2) sia stabile, che lo spanning-tree venga eseguito correttamente e che non vi siano frequenti calcoli dello spanning-tree e modifiche della topologia.

- Il protocollo di routing utilizzato deve inoltre assicurare una convergenza e una stabilità rapide. I fast timer OSPF (Open Shortest Path First) o il protocollo EIGRP (Enhanced Interior Gateway Routing Protocol) sono una buona scelta per questo tipo di rete.

- Usare sempre almeno due interfacce dati sul WSA: uno rivolto ai computer degli utenti finali e un altro destinato al funzionamento in uscita (connesso al proxy upstream o a Internet). Questa operazione viene eseguita per eliminare possibili vincoli di risorse, ad esempio quando il numero di porte TCP è esaurito o quando i buffer di rete sono pieni (in particolare con l'uso di una singola interfaccia sia per l'interno che per l'esterno).

- Per aumentare la sicurezza, dedicare l'interfaccia di gestione al traffico di sola gestione. Per ottenere questo risultato dalla GUI, selezionare **Network > Interfaces** (Rete > Interfacce) e selezionare la casella di controllo **Separate routing (porta M1 limitata solo ai servizi di gestione degli accessori)**.

- Utilizzare server DNS veloci. Qualsiasi transazione tramite WSA richiede almeno una ricerca DNS (se non presente nella cache). Un server DNS lento o che si comporta in modo non corretto influisce su qualsiasi transazione e viene considerato come una connessione Internet ritardata o lenta.

- Quando si utilizzano tabelle di routing separate, si applicano le regole seguenti:

  Tutte le interfacce sono incluse nella tabella di routing di *gestione* predefinita (M1, P1, P2).

  Nella tabella di routing *dei dati* sono incluse solo le interfacce *dati*.

  Nota: La separazione delle tabelle di routing non viene effettuata per interfaccia, bensì per

servizio. Ad esempio, il traffico tra WSA e il controller di dominio Microsoft Active Directory (AD) rispetta sempre le route specificate nella tabella di routing di gestione ed è possibile configurare le route che puntano all'esterno dell'interfaccia P1/P2 in questa tabella. Non è possibile includere route nella tabella di routing dei dati che utilizzano le interfacce di gestione.

Bilanciamento del carico

Di seguito sono riportate alcune considerazioni sul bilanciamento del carico che è possibile implementare per garantire il miglior comportamento della rete:

- Rotazione DNS: termine utilizzato quando un singolo nome host viene utilizzato come proxy, ma dispone di più record A nel server DNS. Ogni client risolve questo problema in un indirizzo IP diverso e utilizza proxy diversi. Una limitazione consiste nel fatto che le modifiche dei record DNS si riflettono sui client al riavvio (cache DNS locale), pertanto offre un basso livello di affidabilità se è necessario apportare una modifica. Tuttavia, ciò è trasparente per gli utenti finali.

- File di controllo dell'indirizzo proxy (PAC) - Si tratta di file di script proxy-automatici che determinano la modalità di gestione di ogni URL su un browser in base alle funzioni scritte al suo interno. Consente di inoltrare sempre lo stesso URL direttamente o allo stesso proxy.

- Rilevamento automatico: descrive l'utilizzo dei metodi DNS/DHCP per ottenere i file PAC (descritti nella considerazione precedente). Di solito, queste prime tre considerazioni sono combinate in un'unica soluzione. Tuttavia, questa operazione può essere complicata e molti agenti utente, come Microsoft Office, Adobe Downloader, Javascripts e Flash, non sono in grado di leggere i file PAC.

- Protocollo WCCP (Web Cache Control Protocol) - Questo protocollo (in particolare WCCP versione 2) costituisce un modo solido e potente per creare il bilanciamento del carico tra diverse WSA e incorporare anche l'alta disponibilità.

- Appliance di bilanciamento del carico separate: Cisco consiglia di utilizzare i load balancing come macchine dedicate.

Firewall

Di seguito sono riportate alcune considerazioni relative al firewall che è possibile implementare per garantire il miglior comportamento della rete:

- Verificare che il protocollo ICMP (Internet Control Message Protocol) sia consentito in tutta la rete da ogni origine. Questo è fondamentale, in quanto il WSA dipende dal meccanismo di rilevamento dell'MTU (Maximum Transition Unit) del percorso, come descritto nella RFC 1191, che dipende dalle richieste Echo ICMP (tipo �� e risposte Echo (tipo 0), ed è richiesta la frammentazione ICMP irraggiungibile (tipo 3, codice 4). Se si disabilita il rilevamento dell'MTU del percorso sul server WSA con il comando **path-mtudiscovery** CLI, il server WSA utilizza la MTU predefinita di 576 byte, come mostrato nella RFC 879. Il problema si ripercuote sulle prestazioni a causa dell'aumento del sovraccarico e del riassemblaggio dei pacchetti.

- Assicurarsi che non vi sia alcun routing asimmetrico all'interno della rete. Anche se non è un problema nel WSA, qualsiasi firewall rilevato lungo il percorso scarta i pacchetti perché non ha ricevuto entrambi i lati della comunicazione.

- Con i firewall, è molto importante escludere gli indirizzi IP WSA dalle minacce come normali stazioni terminali dei computer. Il firewall potrebbe bloccare
- gli indirizzi IP WSA a causa di troppe connessioni (come da conoscenza generale del firewall).

- Se Network Address Translation (NAT) viene utilizzato per qualsiasi indirizzo IP WSA sul dispositivo locale del cliente, verificare che ogni WSA utilizzi un indirizzo globale esterno separato nel NAT. Se si utilizza NAT per più WSA con un unico indirizzo globale esterno, potrebbero verificarsi i problemi seguenti:

  Tutte le connessioni da tutte le WSA al mondo esterno utilizzano un unico indirizzo globale esterno e il firewall esaurisce rapidamente le risorse.

  Se si verifica un picco di traffico verso la singola destinazione, il server di destinazione potrebbe bloccarla e impedire all'intera organizzazione di accedere a questa risorsa. Questa potrebbe essere una risorsa preziosa come lo storage aziendale Cloud, le connessioni Office Cloud o gli aggiornamenti software antivirus per computer.

Identità

Ricorda che il principio *logico AND* si applica a tutte le componenti dell'identità. Ad esempio, se si configurano sia l'agente utente che l'indirizzo IP, l'agente utente verrà identificato *da* questo indirizzo IP. Non indica l'agente utente *o* questo indirizzo IP.

Utilizzare un'identità per l'autenticazione dello stesso tipo di surrogato (o non di surrogato) e/o agente utente.

Èimportante assicurarsi che ogni identità che richiede l'autenticazione includa le stringhe agente utente per i browser/agenti utente noti che supportano l'autenticazione proxy, come Internet Explorer, Mozilla Firefox e Google Chrome. Alcune applicazioni richiedono l'accesso a Internet ma non supportano l'autenticazione proxy/WWW.

Le identità vengono associate dall'alto verso il basso con la ricerca delle corrispondenze che termina con la prima voce corrispondente. Per questo motivo, se sono state configurate le opzioni *Identità 1* e *Identità 2* e una transazione corrisponde all'identità 1, non viene confrontata con l'identità 2.

Criteri accesso/decrittografia/routing/malware in uscita

Questi criteri vengono applicati a diversi tipi di traffico:

- I criteri di accesso vengono applicati alle normali connessioni HTTP o FTP. Determinano se la transazione deve essere accettata o eliminata.

- I criteri di decrittografia determinano se le transazioni HTTPS devono essere decrittografate, eliminate o passate. Se la transazione viene decrittografata, la parte consecutiva può essere considerata come una semplice richiesta HTTP e viene confrontata con i criteri di accesso. Se è necessario eliminare una richiesta HTTPS, eliminarla nei criteri di decrittografia e non nei criteri di accesso. In caso contrario, consuma più CPU e memoria per una transazione eliminata prima da decrittografare e poi da eliminare.

- I criteri di routing determinano la direzione a monte di una transazione dopo che questa è stata consentita tramite WSA. Ciò si verifica se sono presenti proxy a monte o se il server WSA è in modalità *Connector* e invia il traffico al tower Cloud Web Security.

- I criteri malware in uscita vengono applicati ai caricamenti HTTP o FTP da parte degli utenti finali verso i server Web. In genere, si tratta di una richiesta HTTP Post.

Per ogni tipo di politica, è importante ricordare che si applica il principio *logico OR*. Se si fa riferimento a più identità, la transazione deve corrispondere a una qualsiasi delle identità configurate.

Per un controllo più granulare, utilizzare questi criteri. La configurazione errata delle identità per criterio può creare problemi, in cui è più vantaggioso utilizzare più identità a cui si fa riferimento in un criterio. Tenere presente che le identità non influiscono sul traffico, ma si limitano a identificare i tipi di traffico per le corrispondenze successive in una regola.

Spesso i criteri di decrittografia utilizzano identità con l'autenticazione. Sebbene ciò non sia errato e talvolta sia necessario, l'utilizzo di un'identità con l'autenticazione a cui viene fatto riferimento nei criteri di decrittografia significa che tutte le transazioni che corrispondono ai criteri di decrittografia vengono decrittografate per consentire l'autenticazione. È possibile che l'azione di decrittografia venga interrotta o passata, ma poiché esiste un'identità con l'autenticazione, la decrittografia viene eseguita per consentire il passaggio o la caduta del traffico in un secondo momento. Questo è costoso e dovrebbe essere evitato.

Sono state osservate alcune configurazioni che contengono 30 o più identità e 30 o più criteri di accesso, in cui tutti i criteri di accesso includono tutte le identità. In questo caso, non è necessario utilizzare queste numerose identità se corrispondono in tutti i criteri di Access. Anche se ciò non danneggia il funzionamento dell'accessorio, crea confusione con i tentativi di risoluzione dei problemi ed è costoso in termini di prestazioni.

Categorie URL personalizzate

L'utilizzo di categorie URL personalizzate è uno strumento potente disponibile sul Web che viene generalmente frainteso e utilizzato in modo improprio. Ad esempio, esistono configurazioni che contengono tutti i siti video per le corrispondenze nell'identità. WSA dispone di uno strumento integrato che si aggiorna automaticamente quando i siti video cambiano gli URL, il che si verifica di frequente. Pertanto, è opportuno consentire all'amministratore di WSA di gestire le categorie URL automaticamente e di utilizzare le categorie URL personalizzate per siti speciali non ancora classificati.

Prestare particolare attenzione alle espressioni regolari. Se si utilizzano caratteri speciali come il punto (.) e la stella (*), è possibile che la CPU e la memoria siano molto estese. WSA espande qualsiasi espressione regolare per farla corrispondere a ciascuna transazione. Di seguito è riportata, ad esempio, un'espressione regolare:

```
example.*
```

Questa espressione restituirà qualsiasi URL contenente la parola *example*, non solo il dominio *example.com*. Evitare l'uso di *punto* e *stella* nelle espressioni regolari e utilizzarle solo come ultima risorsa.

Di seguito è riportato un altro esempio di espressione regolare che potrebbe creare problemi:

```
www.example.com
```

Se si utilizza questo esempio nel campo Espressioni regolari, il risultato non sarà solo *www.example.com*, ma anche *www.www3example2com.com*, poiché il punto qui indica *qualsiasi carattere*. Se si desidera trovare solo *www.example.com*, escape the dot:

```
www\.example\.com
```

In questo caso, non è necessario utilizzare la funzionalità Espressioni regolari quando è possibile includerla nel dominio della categoria URL personalizzato con questo formato:

```
www.example.com
```

Antimalware e reputazione

Se è abilitato più di un motore di scansione, considerare anche l'opzione per abilitare la scansione adattiva. La scansione adattiva è un motore potente ma di piccole dimensioni sul WSA che pre-scansiona ogni richiesta e determina il motore completo da utilizzare per analizzare le richieste. Questo aumenta leggermente le prestazioni del WSA.