Web security applicatie, ontwerpgids

Inhoud

Inleiding

Dit document beschrijft hoe u de Cisco web security applicatie (WSA) en de bijbehorende onderdelen kunt ontwerpen voor optimale prestaties.

Achtergrondinformatie

Wanneer u een oplossing voor de WSA ontwerpt, moet u dit zorgvuldig overwegen, niet alleen met betrekking tot de configuratie van het apparaat zelf, maar ook met betrekking tot de bijbehorende netwerkapparaten en hun functies. Elk netwerk is een samenwerking van meerdere apparaten, en als één van hen niet correct aan het netwerk deelneemt, dan zouden de gebruikerservaringen kunnen dalen.

Er zijn twee hoofdcomponenten die in aanmerking moeten worden genomen wanneer u de WSA vormt: de hardware en de software. De hardware bestaat uit twee verschillende typen. De eerste is het fysieke type hardware, zoals de S170, S380 en S680 Series modellen, evenals andere modellen End-of-life (EoL), zoals de S160, S360, S660, S370 en S670 Series modellen. Het andere hardwaretype is virtueel, zoals de S000v, S100v en S300v Series modellen. Het besturingssysteem dat op deze hardware draait, wordt *AsyncOS voor web* genoemd, dat is gebaseerd op FreeBSD in de kern.

WSA biedt proxy-service en scant, inspecteert en categoriseert alle verkeer (HTTP, HTTPS en File Transfer Protocol (FTP). Al deze protocollen draaien boven TCP en vertrouwen sterk op Domain Name System (DNS) voor een goede werking. Om deze redenen is de netwerkgezondheid van essentieel belang voor een goed gebruik van het apparaat en voor de communicatie met verschillende delen van het netwerk, zowel binnen als buiten de bedrijfscontrole.

Ontwerpen

Gebruik de informatie die in deze paragraaf wordt beschreven om de WSA en aanverwante onderdelen te ontwerpen voor optimale prestaties.

Netwerknetwerk

Een foutvrij, snel netwerk is van vitaal belang voor de goede werking van de WSA. Als het netwerk instabiel is, zou de gebruikerservaring kunnen dalen. Netwerkproblemen worden meestal gedetecteerd wanneer webpagina's langer nodig zijn om te bereiken of onbereikbaar zijn. De aanvankelijke neiging is verantwoordelijk voor het apparaat, maar het is meestal het netwerk dat zich slecht gedraagt. Er moet dus zorgvuldig worden nagedacht en gecontroleerd om te waarborgen dat het netwerk de beste service biedt voor toepassingsprotocollen op hoog niveau zoals HTTP, HTTPS, FTP en DNS.

Algemene overwegingen

Hier zijn een paar algemene overwegingen die u kunt implementeren om het beste netwerkgedrag te verzekeren:

- Verzeker dat het netwerk van Layer 2 (L2) stabiel is, dat de overspannende-boom verrichting correct is, en dat er niet vaak overspant-boom berekeningen en topologie veranderingen zijn.

- Het routingprotocol dat wordt gebruikt moet ook snelle convergentie en stabiliteit bieden. De snelle timers Open Shortest Path First (OSPF) of het Enhanced Interior Gateway Routing Protocol (DHCP) zijn goede keuzes voor een dergelijk netwerk.

- Gebruik altijd ten minste twee gegevensinterfaces op de WSA: een die geconfronteerd wordt met de eindgebruikerscomputers en een ander voor uitgaande werking (verbonden met de upstream-proxy of het internet). Dit wordt gedaan om mogelijke resource beperkingen te elimineren, zoals wanneer het aantal TCP poorten is uitgeput of wanneer de netwerkbuffers vol worden (met het gebruik van één enkele interface voor zowel binnen als buiten in het bijzonder).

- Speciale Management-interface voor alleen beheerverkeer om de beveiliging te verhogen. Om dit via de GUI te bereiken, navigeer dan naar **Netwerk > Interfaces** en controleer de **aparte routing (M1 poort alleen beperkt tot** gastelbeheerservices).

- Gebruik snelle DNS-servers. Elke transactie via de WSA vereist ten minste één DNS raadpleging (indien niet in het cache). Een DNS-server die langzaam of slecht werkt, beïnvloedt elke transactie en wordt gezien als een vertraagde of langzame internetverbinding.

- Wanneer afzonderlijke routingtabellen worden gebruikt, zijn deze regels van toepassing:

  Alle interfaces zijn opgenomen in de standaard *Management*-routingtabel (M1, P1, P2).

  In de tabel *Data* Routing wordt alleen een gegevensinterface opgenomen.

  Opmerking: De scheiding van routeringstabellen is niet per interface, maar per service. Bijvoorbeeld, verkeer tussen de WSA en de Microsoft Active Directory (AD) domeincontroller volgt altijd de routes die in de routingtabel van het beheer worden gespecificeerd en het is

mogelijk om routes te configureren die uit de P1/P2 interface in deze tabel wijzen. Het is niet mogelijk om routes in de Data Routing Tabel op te nemen die de Management-interfaces gebruiken.

Taakverdeling

Hier zijn een aantal load-balances overwegingen die u kunt implementeren om het beste netwerkgedrag te verzekeren:

- DNS-draaiing - Dit is de term die wordt gebruikt wanneer één hostname als een proxy wordt gebruikt, maar er zijn meerdere A-records op de DNS-server. Elke client lost dit op tot een ander IP-adres en gebruikt verschillende proxy's. Een beperking is dat veranderingen van DNS-records op klanten worden weerspiegeld na herstart (lokale DNS-caching), zodat deze een lage robuustheid biedt als er een verandering moet worden aangebracht. Dit is echter transparant voor de eindgebruikers.

- Proxy Address Control (PAC)-bestanden - Dit zijn proxy-Automatisch scripting files dat bepalen hoe elke URL op een browser moet worden verwerkt op basis van de geschreven functies erin. Deze heeft de functie om dezelfde URL altijd direct of bij dezelfde proxy door te sturen.

- Automatische detectie - Dit beschrijft het gebruik van DNS/DHCP-methoden om PAC-bestanden te verkrijgen (beschreven in de vorige overweging). Gewoonlijk worden deze eerste drie overwegingen gecombineerd tot één oplossing. Dit kan echter ingewikkeld zijn en veel gebruikersagents, zoals Microsoft Office, Adobe Downloader, Javasverlts en Flash, kunnen PAC-bestanden helemaal niet lezen.

- Web Cache Control Protocol (WCCP) - Dit protocol (met name WCCP, versie 2) biedt een robuuste en zeer krachtige manier om een taakverdeling te maken tussen verschillende WSA's en ook een hoge beschikbaarheid te integreren.

- Aparte taakverdeler(s) - Cisco raadt aan om taakverdelers te gebruiken als speciale machines.

Firewalls

Hier zijn een paar firewalloverwegingen die u kunt implementeren om het beste netwerkgedrag te verzekeren:

- Zorg ervoor dat Internet Control Message Protocol (ICMP) uit elke bron binnen het netwerk is toegestaan. Dit is van vitaal belang, aangezien de WSA afhankelijk is van het ontkenningsmechanisme van de Path Max Transition Unit (MTU), zoals beschreven in RFC 1191, dat afhangt van verzoeken van ICMP Echo (type ⁄⁄ en Echo-antwoorden (type 0), en het ICMP is vereist van onbereikbare fragmentatie (type 3, code 4). Als u pad MTU discovery op het WSA uitschakelt met de opdracht **pathmutdiscovery** CLI, dan gebruikt de WSA de standaard MTU van 576 bytes, zoals per RFC 879. Dit beïnvloedt de prestaties door verhoogde overhead en een hermontage van pakketten.

- Zorg ervoor dat er geen asymmetrische routing binnen het netwerk is. Hoewel dit geen probleem is op de WSA, laat elke Firewall die langs het pad wordt aangetroffen de pakketten vallen omdat deze beide kanten van de communicatie niet heeft ontvangen.

- Met Firewalls is het zeer belangrijk de WSA IP-adressen van bedreigingen als reguliere eindcomputerstations uit te sluiten. De firewall kan blokkeren
- de WSA IP-adressen door te veel verbindingen (zoals bij algemene firewallkennis).

- Als Network Address Translation (NAT) wordt gebruikt voor een WSA IP-adres op het apparaat van de klant, zorg er dan voor dat elke WSA een afzonderlijk extern mondiaal adres in het NAT gebruikt. Als u NAT gebruikt voor meerdere WSA's die één enkel extern mondiaal adres hebben, zou u deze kwesties kunnen ontmoeten:

  Alle verbindingen van alle WSA's naar de buitenwereld gebruiken één enkel extern mondiaal adres, en de Firewall raakt snel uit zijn middelen.

  Als er een toename van verkeer naar die ene bestemming is, kan de doelserver het blokkeren en de gehele onderneming van de toegang tot deze bron uitsluiten. Dit kan een waardevolle bron zijn zoals de Cloud-opslag van het bedrijf, de Office Cloud-verbindingen of de antivirusupdates per computer.

Identiteiten

Onthoud dat het *logische EN* principe van toepassing is op alle componenten van de identiteit. Als u bijvoorbeeld zowel het user-agent- als IP-adres configureren betekent dit de gebruikersagent *van* dit IP-adres. Dit betekent niet de gebruikersagent *of* dit IP-adres.

Gebruik één identiteit voor authenticatie van hetzelfde surrogaat type (of geen surrogaat) en/of gebruikersagent.

Het is belangrijk om ervoor te zorgen dat elke identiteit waarvoor verificatie nodig is, ook de gebruikersagent strings bevat voor bekende browsers/gebruikers-agenten die proxy-verificatie ondersteunen, zoals Internet Explorer, Mozilla Firefox en Google Chrome. Er zijn bepaalde toepassingen die internettoegang vereisen maar geen proxy/WW verificatie ondersteunen.

Identificaties worden van boven naar onder aangepast met de zoekopdracht naar overeenkomsten die eindigen bij de eerste gematchte ingang. Om deze reden wordt, als u *Identity 1* en *Identity 2* hebt ingesteld en een transactie overeenkomt met Identity 1, niet ingeschakeld tegen Identity 2.

Beleid inzake toegang/decryptie/routing/Outbound Malware

Dit beleid wordt toegepast op verschillende soorten verkeer:

- Toegangsbeleid wordt toegepast tegen gewone HTTP- of FTP-verbindingen. Zij bepalen of de transactie moet worden aanvaard of ingetrokken.

- Decryptie beleid bepaalt of HTTPS-transacties moeten worden gedecrypteerd, gedropt of doorgegeven. Als de transactie wordt gedecrypteerd, dan kan het achtereenvolgende deel

ervan als een pure HTTP aanvraag worden gezien en tegen beleid van de Toegang worden aangepast. Als u een HTTPS-aanvraag moet laten vallen, laat u deze in het decryptiebeleid vallen, niet in het toegangsbeleid. Anders verbruikt het meer CPU en geheugen voor een geworpen transactie, eerst gedecrypteerd en daarna te laten vallen.

- Routing beleid bepaalt de stroomopwaartse richting van een transactie zodra deze door de WSA is toegestaan. Dit is van toepassing als er stroomopwaartse proxy's zijn of als de WSA in Connectormodus is en verkeer naar de Cloud Web Security Toren verstuurt.

- Uitgaande malware-beleid wordt toegepast tegen HTTP- of FTP-uploads van eindgebruikers naar webservers. Dit wordt meestal gezien als een HTTP Post-aanvraag.

Voor elk type beleid is het belangrijk te bedenken dat het *logische OF OF*-beginsel van toepassing is. Als u meerdere identiteiten hebt doorverwezen, moet de transactie om het even welke identiteiten overeenkomen die worden gevormd.

Gebruik dit beleid voor een meer gedetailleerde controle. Onjuist samengestelde identiteiten per beleid kunnen problemen creëren, waar het voordeliger is om verschillende identiteiten te gebruiken waarnaar in een beleid wordt verwezen. Vergeet niet dat identiteiten het verkeer niet beïnvloeden, ze identificeren alleen de soorten verkeer voor latere wedstrijden in een beleid.

Vaak gebruiken decryptie beleid identiteiten met authenticatie. Hoewel dit niet verkeerd is en soms nodig is, betekent het gebruik van een identiteit met authenticatie waarnaar in het decryptiebeleid wordt verwezen dat alle transacties die overeenkomen met het decryptiebeleid worden decryptie-gedecrypteerd om de authenticatie te laten plaatsvinden. De decryptie-actie kan vallen of doorlopen, maar aangezien er een identiteit is met authenticatie, vindt de decryptie plaats om later door het verkeer te laten vallen of passeren. Dit is duur en moet worden vermeden.

Sommige configuraties zijn waargenomen die 30 of meer identiteiten en 30 of meer toegangsbeleid bevatten, waarbij al het toegangsbeleid alle identiteiten omvat. In dit geval hoeft dit getal niet gebruikt te worden als het overeenkomt met het volledige toegangsbeleid. Hoewel dit de werking van het apparaat niet nadelig beïnvloedt, creëert het verwarring met pogingen om problemen op te lossen en is het duur wat de prestaties betreft.

Aangepaste URL-categorieën

Het gebruik van aangepaste URL-categorieën is een krachtig gereedschap in de WSA dat gewoonlijk verkeerd wordt begrepen en gebruikt. Bijvoorbeeld, er zijn configuraties die alle videoplaatsen voor overeenkomsten in de identiteit bevatten. De WSA heeft een ingebouwde gereedschap dat automatisch updates wanneer videoplaatsen URLs veranderen, die vaak voorkomen. Daarom is het verstandig om WSA toe te staan om de URL categorieën automatisch te beheren, en de aangepaste URL categorieën voor speciale, nog niet gecategoriseerde plaatsen te gebruiken.

Wees erg voorzichtig met reguliere expressies. Als speciale tekens zoals punt (.) en ster(*) worden gebruikt, kunnen deze zeer CPU's- en geheugenextensies opleveren. WSA breidt elke reguliere expressie uit om deze met elke transactie aan te passen. Hier is bijvoorbeeld een reguliere expressie:

```
example.*
```

Deze expressie komt overeen met elke URL die het woord *voorbeeld* bevat, en niet alleen het

voorbeeld.com-domein. Vermijd het gebruik van *stip* en *ster* in reguliere expressies en gebruik ze alleen in laatste instantie.

Hier is een ander voorbeeld van een reguliere expressie die problemen kan veroorzaken:

```
www.example.com
```

Als u dit voorbeeld in het veld Reguliere expressies gebruikt, komt deze niet alleen overeen met *www.example.com*, maar ook met *www.www3example2com.com*, omdat de stip hier *elk teken* betekent. Als u alleen *www.example.com* wilt vergelijken, ontsnapt u aan de punt:

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

In dit geval is er geen reden om de optie Reguliere expressies te gebruiken wanneer u dit in het aangepaste URL-categoriedomein met deze notatie kunt opnemen:

```
www.example.com
```

Anti-Malware en reputatie

Als er meer dan één scanmachine is ingeschakeld, raadpleegt u de optie om ook het adaptieve scannen mogelijk te maken. Adaptieve scannen is een krachtige maar kleine motor in de WSA die elk verzoek vooraf scant en de volledige motor bepaalt die moet worden gebruikt om verzoeken te scannen. Dit verhoogt de prestaties op de WSA licht.