Designleitfaden für Web Security Appliance

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie die Cisco Web Security Appliance (WSA) und die zugehörigen Komponenten für eine optimale Leistung entworfen werden.

Hintergrundinformationen

Wenn Sie eine Lösung für die WSA entwerfen, muss diese sorgfältig geprüft werden, nicht nur hinsichtlich der Konfiguration der Appliance selbst, sondern auch hinsichtlich der zugehörigen Netzwerkgeräte und ihrer Funktionen. Jedes Netzwerk besteht aus einer Zusammenarbeit mit mehreren Geräten. Wenn eines dieser Geräte nicht ordnungsgemäß am Netzwerk teilnimmt, kann das Benutzererlebnis sinken.

Beim Konfigurieren der WSA müssen zwei Hauptkomponenten beachtet werden: Hardware und Software. Die Hardware ist in zwei verschiedene Typen erhältlich. Der erste Typ ist die physische Hardware, z. B. die Modelle der Serien S170, S380 und S680 sowie andere EoL-Modelle, wie die Modelle der Serien S160, S360, S660, S370 und S670. Der andere Hardwaretyp ist virtuell, z. B. die Modelle der Serien S000v, S100v und S300v. Das Betriebssystem, das auf dieser Hardware ausgeführt wird, heißt *AsyncOS für Web*, das auf FreeBSD basiert.

Die WSA bietet Proxydienste und scannt, prüft und kategorisiert außerdem den gesamten Datenverkehr (HTTP, HTTPS und File Transfer Protocol (FTP)). Alle diese Protokolle werden über TCP ausgeführt und basieren im Hinblick auf den ordnungsgemäßen Betrieb in hohem Maße auf Domain Name System (DNS). Aus diesen Gründen ist die Netzwerkintegrität für den ordnungsgemäßen Betrieb der Appliance und ihre Kommunikation mit verschiedenen Teilen des Netzwerks, sowohl innerhalb als auch außerhalb der Unternehmenssteuerung, unerlässlich.

Design

Verwenden Sie die in diesem Abschnitt beschriebenen Informationen, um die WSA und die

zugehörigen Komponenten für eine optimale Leistung zu entwickeln.

Netzwerk

Ein fehlerfreies, schnelles Netzwerk ist für den ordnungsgemäßen Betrieb der WSA unerlässlich. Wenn das Netzwerk instabil ist, kann die Benutzerfreundlichkeit abnehmen. Netzwerkprobleme werden in der Regel erkannt, wenn Webseiten länger oder nicht erreichbar sind. Die anfängliche Neigung ist die Schuld an der Appliance, aber es ist normalerweise das Netzwerk, das sich falsch verhält. Daher sollte sorgfältig geprüft und geprüft werden, um sicherzustellen, dass das Netzwerk den besten Service für High-Level-Anwendungsprotokolle wie HTTP, HTTPS, FTP und DNS bietet.

Allgemeine Überlegungen

Hier einige allgemeine Überlegungen, die Sie implementieren können, um das beste Netzwerkverhalten sicherzustellen:

- Stellen Sie sicher, dass das Layer-2-Netzwerk (L2) stabil ist, dass der Spanning-Tree-Betrieb korrekt ist und dass es keine häufigen Spanning-Tree-Berechnungen und Topologieänderungen gibt.

- Das verwendete Routing-Protokoll sollte außerdem eine schnelle Konvergenz und Stabilität bieten. Die OSPF-Timer (Open Shortest Path First) oder das EIGRP (Enhanced Interior Gateway Routing Protocol) sind eine gute Wahl für ein solches Netzwerk.

- Verwenden Sie immer mindestens zwei Datenschnittstellen auf der WSA: eine für die Endbenutzercomputer und eine für den ausgehenden Betrieb (verbunden mit dem Upstream-Proxy oder dem Internet). Dies geschieht, um mögliche Ressourceneinschränkungen zu vermeiden, z. B. wenn die Anzahl der TCP-Ports erschöpft ist oder wenn die Netzwerkpuffer voll werden (insbesondere bei Verwendung einer einzigen Schnittstelle für innen und außen).

- Dedizieren Sie die Management-Schnittstelle für reinen Management-Datenverkehr, um die Sicherheit zu erhöhen. Um dies über die GUI zu erreichen, navigieren Sie zu **Network > Interfaces (Netzwerk > Schnittstellen),** und aktivieren Sie das **Kontrollkästchen Separate Routing (M1-Port ist nur auf Appliance Management Services beschränkt)**.

- Schnelle DNS-Server verwenden. Jede Transaktion über die WSA erfordert mindestens eine DNS-Suche (wenn nicht im Cache). Ein DNS-Server, der langsam ist oder sich falsch verhält, wirkt sich auf alle Transaktionen aus und wird als verzögerte oder langsame Internetverbindung beobachtet.

- Bei Verwendung separater Routing-Tabellen gelten folgende Regeln:

  Alle Schnittstellen sind in der Standard-*Management*-Routing-Tabelle (M1, P1, P2) enthalten.

  In der *Data* Routing-Tabelle sind nur Datenschnittstellen enthalten.

  Hinweis: Die Trennung der Routing-Tabellen erfolgt nicht pro Schnittstelle, sondern pro Service. Beispielsweise befolgen der Datenverkehr zwischen der WSA und dem Microsoft

Active Directory (AD)-Domänencontroller immer die in der Management-Routing-Tabelle angegebenen Routen. Außerdem ist es möglich, Routen zu konfigurieren, die auf die P1/P2-Schnittstelle in dieser Tabelle hinweisen. Routen, die die Management-Schnittstellen verwenden, können nicht in die Data Routing-Tabelle aufgenommen werden.

Lastenausgleich

Im Folgenden sind einige Überlegungen zum Lastenausgleich aufgeführt, die Sie implementieren können, um ein optimales Netzwerkverhalten sicherzustellen:

- DNS-Rotation - Dieser Begriff wird verwendet, wenn ein einzelner Hostname als Proxy verwendet wird, aber mehrere A-Datensätze auf dem DNS-Server vorhanden sind. Jeder Client löst dies in eine andere IP-Adresse auf und verwendet verschiedene Proxys. Eine Einschränkung besteht darin, dass Änderungen von DNS-Datensätzen bei einem Neustart (lokales DNS-Caching) auf den Clients reflektiert werden. Wenn eine Änderung vorgenommen werden muss, ist die Robustheit daher gering. Dies ist jedoch für die Endbenutzer transparent.

- Proxy Address Control (PAC)-Dateien - Hierbei handelt es sich um Proxy-automatische Skriptdateien, die festlegen, wie jede URL auf der Grundlage der darin enthaltenen geschriebenen Funktionen in einem Browser behandelt werden soll. Es hat die Funktion, immer die gleiche URL direkt oder an den gleichen Proxy weiterzuleiten.

- Automatische Erkennung - Dies beschreibt die Verwendung von DNS-/DHCP-Methoden, um PAC-Dateien abzurufen (wie im vorherigen Abschnitt beschrieben). In der Regel werden diese ersten drei Überlegungen zu einer Lösung zusammengefasst. Dies kann jedoch kompliziert sein, und viele Benutzeragenten wie Microsoft Office, Adobe Downloader, JavaScript und Flash können PAC-Dateien überhaupt nicht lesen.

- Web Cache Control Protocol (WCCP) - Dieses Protokoll (insbesondere WCCP Version 2) bietet eine robuste und sehr leistungsstarke Möglichkeit zum Erstellen von Lastenausgleich zwischen mehreren WSAs und zum Integrieren von Hochverfügbarkeit.

- Separate Load Balancing-Appliance(s): Cisco empfiehlt, Load Balancer als dedizierte Systeme zu verwenden.

Firewalls

Hier einige Überlegungen zur Firewall, die Sie implementieren können, um ein optimales Netzwerkverhalten sicherzustellen:

- Stellen Sie sicher, dass Internet Control Message Protocol (ICMP) im gesamten Netzwerk von jeder Quelle zugelassen ist. Dies ist von entscheidender Bedeutung, da die WSA vom Mechanismus der MTU-Erkennung (Maximum Transition Unit) des Pfads abhängig ist, wie in RFC 1191 beschrieben, der von ICMP-Echo-Anfragen (Typ ⓪ und Echo-Antworten (Typ 0)) abhängt, und eine ICMP-Fragmentierung ohne Erreichbarkeit (Typ 3, Code 4) erforderlich ist. Wenn Sie die MTU-Pfaderkennung auf der WSA mithilfe des CLI-Befehls **pathmtudiscovery** deaktivieren, verwendet die WSA die Standard-MTU von 576 Byte gemäß RFC 879. Dies

wirkt sich auf die Leistung aus, da der Overhead steigt und Pakete neu zusammengesetzt werden.

- Stellen Sie sicher, dass im Netzwerk kein asymmetrisches Routing vorhanden ist. Obwohl dies kein Problem bei der WSA darstellt, verwirft jede Firewall, die entlang des Pfads angetroffen wird, die Pakete, da sie nicht beide Seiten der Kommunikation empfangen hat.

- Bei Firewalls ist es sehr wichtig, die WSA-IP-Adressen als reguläre Endcomputer-Stationen von Bedrohungen auszuschließen. Die Firewall kann blockieren.
- die WSA-IP-Adressen aufgrund zu vieler Verbindungen (gemäß allgemeiner Firewall-Kenntnisse).

- Wenn Network Address Translation (NAT) für eine beliebige WSA-IP-Adresse auf dem Gerät des Kunden verwendet wird, stellen Sie sicher, dass jede WSA eine separate externe globale Adresse in der NAT verwendet. Wenn Sie NAT für mehrere WSAs mit einer einzigen externen globalen Adresse verwenden, können folgende Probleme auftreten:

  Alle Verbindungen von allen WSAs nach außen verwenden eine einzige externe globale Adresse, und der Firewall werden schnell die Ressourcen erschöpft.

  Wenn ein Anstieg des Datenverkehrs zu diesem einzelnen Ziel auftritt, kann der Zielserver diesen blockieren und den Zugriff des gesamten Unternehmens auf diese Ressource unterbinden. Dies kann eine wertvolle Ressource sein, z. B. das Unternehmen Cloud Storage, die Office Cloud-Verbindungen oder die Computer-basierten Antivirus-Software-Updates.

Identitäten

Denken Sie daran, dass das *logische UND* Prinzip in allen Komponenten der Identität gilt. Wenn Sie z. B. sowohl den Benutzer-Agent als auch die IP-Adresse konfigurieren, bedeutet dies, dass der Benutzer-Agent *von* dieser IP-Adresse aus besteht. Dies bezieht sich nicht auf den Benutzer-Agent *oder* diese IP-Adresse.

Verwenden Sie eine Identität für die Authentifizierung desselben Ersatzteiltyps (oder ohne Ersatzzeichen) und/oder Benutzeragenten.

Es ist wichtig sicherzustellen, dass jede Identität, die authentifiziert werden muss, die Benutzer-Agent-Zeichenfolgen für bekannte Browser/Benutzer-Agents enthält, die Proxy-Authentifizierung unterstützen, z. B. Internet Explorer, Mozilla Firefox und Google Chrome. Einige Anwendungen erfordern Internetzugriff, unterstützen jedoch keine Proxy-/WWW-Authentifizierung.

Identitäten werden von oben nach unten mit der Suche nach Übereinstimmungen zugeordnet, die am ersten zugeordneten Eintrag enden. Wenn Sie aus diesem Grund *Identity 1* und *Identity 2* konfiguriert haben und eine Transaktion mit Identity 1 übereinstimmt, wird sie nicht mit Identity 2 (Identität 2) verglichen.

Zugriffs-/Entschlüsselungs-/Routing-/Richtlinien für ausgehende Malware

Diese Richtlinien werden auf verschiedene Arten von Datenverkehr angewendet:

- Zugriffsrichtlinien werden auf einfache HTTP- oder FTP-Verbindungen angewendet. Sie legen fest, ob die Transaktion akzeptiert oder abgebrochen werden soll.

- Entschlüsselungsrichtlinien legen fest, ob HTTPS-Transaktionen entschlüsselt, verworfen oder übergeben werden sollen. Wenn die Transaktion entschlüsselt wird, kann der folgende Teil als einfache HTTP-Anforderung angesehen werden und wird mit den Zugriffsrichtlinien abgeglichen. Wenn Sie eine HTTPS-Anforderung verwerfen müssen, geben Sie sie in die Entschlüsselungsrichtlinien und nicht in die Zugriffsrichtlinien ein. Andernfalls benötigt es mehr CPU und Arbeitsspeicher, damit eine gelöschte Transaktion zuerst entschlüsselt und dann verworfen wird.

- Routing-Richtlinien bestimmen die Upstream-Richtung einer Transaktion, sobald sie durch die WSA zulässig ist. Dies gilt, wenn Upstream-Proxys vorhanden sind oder sich die WSA im *Connector*-Modus befindet und Datenverkehr an den Cloud Web Security-Tower sendet.

- Richtlinien für ausgehende Malware werden für HTTP- oder FTP-Uploads von Endbenutzern auf Webserver angewendet. Dies wird in der Regel als HTTP-Post-Anfrage angezeigt.

Für jeden Richtlinientyp ist es wichtig zu beachten, dass das *logische OR*-Prinzip gilt. Wenn Sie mehrere Identitäten verweisen, sollte die Transaktion einer der konfigurierten Identitäten entsprechen.

Verwenden Sie diese Richtlinien, um eine genauere Kontrolle zu erhalten. Falsch konfigurierte Identitäten pro Richtlinie können Probleme verursachen, wenn es vorteilhafter ist, mehrere Identitäten zu verwenden, auf die in einer Richtlinie verwiesen wird. Beachten Sie, dass Identitäten keinen Einfluss auf den Datenverkehr haben. Sie identifizieren lediglich die Datenverkehrstypen für spätere Übereinstimmungen in einer Richtlinie.

Entschlüsselungsrichtlinien verwenden häufig Identitäten mit Authentifizierung. Obwohl dies nicht falsch ist und manchmal erforderlich ist, bedeutet die Verwendung einer Identität mit Authentifizierung, auf die in der Entschlüsselungsrichtlinie verwiesen wird, dass alle Transaktionen, die der Entschlüsselungsrichtlinie entsprechen, entschlüsselt werden, damit die Authentifizierung erfolgt. Die Entschlüsselungsaktion kann verworfen oder durchlaufen werden. Da jedoch eine Identität mit Authentifizierung vorhanden ist, findet die Entschlüsselung statt, um den Datenverkehr später zu verwerfen oder zu durchlaufen. Das ist teuer und sollte vermieden werden.

Es wurden einige Konfigurationen beobachtet, die mindestens 30 Identitäten und mindestens 30 Zugriffsrichtlinien enthalten, in denen alle Zugriffsrichtlinien alle Identitäten enthalten. In diesem Fall müssen diese vielen Identitäten nicht verwendet werden, wenn sie in allen Zugriffsrichtlinien zugeordnet werden. Dies schadet zwar nicht dem Betrieb der Appliance, führt jedoch zu Verwirrung bei Fehlerbehebungsversuchen und ist in Bezug auf die Leistung kostspielig.

Benutzerdefinierte URL-Kategorien

Die Verwendung benutzerdefinierter URL-Kategorien ist ein leistungsstarkes Tool auf der WSA, das in der Regel missverstanden und missbraucht wird. Es gibt z. B. Konfigurationen, die alle Video-Sites für Übereinstimmungen in der Identität enthalten. Die WSA verfügt über ein integriertes Tool, das automatisch aktualisiert wird, wenn Videostandorte URLs ändern, was häufig vorkommt. Daher ist es sinnvoll, der WSA zu gestatten, die URL-Kategorien automatisch zu verwalten und die benutzerdefinierten URL-Kategorien für spezielle, noch nicht kategorisierte

Sites zu verwenden.

Seien Sie sehr vorsichtig mit regulären Ausdrücken. Wenn Sonderzeichenfolgen wie Punkt (.) und Stern(*) verwendet werden, können sich diese als sehr CPU- und speicherintensiv erweisen. Die WSA erweitert jeden regulären Ausdruck, um ihn mit jeder Transaktion abzugleichen. Hier ist beispielsweise ein regulärer Ausdruck:

```
example.*
```

Dieser Ausdruck entspricht einer beliebigen URL, die das Wort *example* enthält, nicht nur der *example.com*-Domäne. Vermeiden Sie die Verwendung von *Punkten* und *Sternen* in regulären Ausdrücken und verwenden Sie diese nur als letzte Möglichkeit.

Hier ist ein weiteres Beispiel für einen regulären Ausdruck, der Probleme verursachen könnte:

```
www.example.com
```

Wenn Sie dieses Beispiel im Feld Reguläre Ausdrücke verwenden, entspricht es nicht nur *www.example.com*, sondern auch *www.www3example2com.com*, da der Punkt hier *ein beliebiges Zeichen* bedeutet. Wenn Sie nur *www.example.com* übereinstimmen möchten, müssen Sie den folgenden Punkt entfernen:

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

In diesem Fall gibt es keinen Grund, die Funktion Reguläre Ausdrücke zu verwenden, wenn Sie diese in die benutzerdefinierte URL-Kategoriendomäne mit folgendem Format einschließen können:

```
www.example.com
```

Anti-Malware und Reputation

Wenn mehrere Scan-Engines aktiviert sind, können Sie auch adaptive Scans aktivieren. Adaptives Scanning ist eine leistungsstarke, aber kleine Engine auf der WSA, die jede Anforderung vorab scannt und die umfassende Engine bestimmt, die zum Scannen von Anfragen verwendet werden soll. Dadurch wird die Leistung der WSA leicht erhöht.