Cisco-gids voor Harden Cisco ASA-firewall

Inhoud

Inleiding

Dit document bevat informatie om u te helpen Cisco ASA-apparaten te beveiligen, wat de algemene beveiliging van uw netwerk verhoogt. Dit document is opgebouwd uit 4 afdelingen

Hardnekkig beheersplan - Dit is van toepassing op alle ASA-gerelateerde Management/To-the box-verkeer zoals SNMP,SSH enzovoort.
Beveiliging van een **configuratie** - Opdrachten waardoor we kunnen stoppen met het bevolken van de wachtwoorden etc. voor de actieve configuratie enzovoort
Vastlegging en bewaking - Dit is van toepassing op alle instellingen met betrekking tot houtkap op ASA.
Door verkeer - Dit is van toepassing op het verkeer dat door de ASA gaat.

De dekking van de veiligheidseigenschappen in dit document verstrekt vaak genoeg detail om de eigenschap te configureren. Indien dit niet het geval is, wordt de functie echter zodanig uitgelegd dat u kunt beoordelen of extra aandacht voor de functie nodig is. Waar mogelijk en passend bevat dit document aanbevelingen die, indien ze worden uitgevoerd, bijdragen tot de beveiliging van een netwerk.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco ASA 5500-X 9.4(1) en hoger.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een

opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Verwante producten

Deze configuratie kan ook worden gebruikt met Cisco ASA 5500-X Series security applicatie, versie 9.x.

Conventies

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

Beveiligingsbewerkingen

Beveiligde netwerkbewerkingen zijn een substantieel onderwerp. Hoewel het meeste van dit document is gewijd aan de veilige configuratie van een Cisco ASA-apparaat, zijn configuraties alleen niet volledig veilig voor een netwerk. De op het netwerk toegepaste operationele procedures dragen evenveel bij tot de veiligheid als de configuratie van de onderliggende apparatuur.

Deze onderwerpen bevatten operationele aanbevelingen die u geadviseerd wordt te implementeren. Deze onderwerpen benadrukken specifieke kritieke gebieden van netwerkoperaties en zijn niet uitgebreid.

Cisco Security Advisories en antwoorden bewaken

Het Cisco Product Security Incident Response Team (PSIRT) maakt en onderhoudt publicaties, vaak PSIRT Advisories, voor security-gerelateerde problemen in Cisco-producten. De methode die wordt gebruikt voor communicatie van minder ernstige problemen is de Cisco Security Response. Security advisories en antwoorden zijn beschikbaar op PSIRT.

Aanvullende informatie over deze communicatievoertuigen is beschikbaar in het Cisco Security kwetsbaarheidsbeleid.

Om een veilig netwerk te onderhouden moet u op de hoogte zijn van de Cisco security adviseurs en de reacties die zijn vrijgegeven. U moet op de hoogte zijn van een kwetsbaarheid voordat de dreiging die het kan vormen voor een netwerk kan worden beoordeeld. Raadpleeg de risicoanalyse voor de kwetsbaarheid van de beveiliging en de aankondigingen voor ondersteuning van dit evaluatieproces.

Levering verificatie, autorisatie en accounting

Het kader voor verificatie, autorisatie en accounting (AAA) is essentieel om netwerkapparaten te beveiligen. Het AAA-kader biedt verificatie van beheersessies en kan gebruikers ook beperken tot specifieke, door een beheerder gedefinieerde opdrachten en alle opdrachten die door alle gebruikers zijn ingevoerd, registreren. Zie het gedeelte Verificatie, autorisatie en accounting van dit document voor meer informatie over hoe u AAA kunt gebruiken.

Gecentraliseerde bestandsverzameling en -bewaking

Om kennis te verwerven over bestaande, opkomende en historische gebeurtenissen die betrekking hebben op veiligheidsincidenten, moet uw organisatie een gezamenlijke strategie hebben voor het registreren van gebeurtenissen en het correleren daarvan. Deze strategie moet de houtkap van alle netwerkapparaten aanvullen en vooraf verpakte en aanpasbare correlatiemogelijkheden gebruiken.

Nadat gecentraliseerde houtkap is geïmplementeerd, moet u een gestructureerde benadering van loganalyse en het opsporen van incidenten ontwikkelen. Gebaseerd op de behoeften van uw organisatie, kan deze benadering variëren van een eenvoudig zorgvuldig onderzoek van loggegevens tot geavanceerde op regelgeving gebaseerde analyse.

Indien mogelijk beveiligde protocollen gebruiken

Veel protocollen worden gebruikt om gevoelige netwerkbeheergegevens over te dragen. U moet waar mogelijk veilige protocollen gebruiken. Een veilige protocolkeuze omvat het gebruik van SSH in plaats van telnet, zodat zowel de authenticatiegegevens als de beheerinformatie worden versleuteld. Daarnaast moet u veilige protocollen voor bestandsoverdracht gebruiken wanneer u configuratiegegevens kopieert. Een voorbeeld is het gebruik van het Secure Copy Protocol (SCP) in plaats van FTP of TFTP.

Gain Traffic Visibility and met NetFlow

Met NetFlow kunt u de verkeersstromen in het netwerk bewaken. Oorspronkelijk bedoeld om verkeersinformatie naar netwerkbeheertoepassingen uit te voeren, kan NetFlow ook worden gebruikt om stroominformatie op een router weer te geven. Deze mogelijkheid stelt u in staat om te zien wat verkeer het netwerk in real time overbrengt. Ongeacht of de stroominformatie naar een afstandsbediening wordt geëxporteerd, wordt u geadviseerd om netwerkapparaten voor NetFlow te configureren zodat deze indien nodig reactief gebruikt kan worden.

Configuratie-beheer

Configuratiebeheer is een proces waarmee configuratiewijzigingen worden voorgesteld, beoordeeld, goedgekeurd en ingezet. Binnen de context van een Cisco ASA-apparaatconfiguratie zijn twee extra aspecten van configuratiebeheer van cruciaal belang: archivering en beveiliging van de configuratie.

U kunt configuratiearchieven gebruiken om veranderingen terug te draaien die aan netwerkapparaten gemaakt worden. In een veiligheidscontext kunnen de configuratie archieven ook worden gebruikt om te bepalen welke beveiligingswijzigingen zijn aangebracht en wanneer deze wijzigingen zich hebben voorgedaan. In combinatie met de loggegevens van AAA kan deze informatie helpen bij de veiligheidscontrole van netwerkapparaten.

De configuratie van een Cisco ASA-apparaat bevat veel gevoelige details. Gebruikersnaam, wachtwoorden en de inhoud van toegangscontrolelijsten zijn voorbeelden van dit type informatie. De opslagplaats die u gebruikt om Cisco ASA-apparaatconfiguraties te archiveren moet beveiligd zijn. Onveilige toegang tot deze informatie kan de veiligheid van het gehele netwerk ondermijnen.

Beheer Vliegtuig

Het beheersvlak bestaat uit functies die de beheersdoelstellingen van het netwerk bereiken. Dit

omvat interactieve beheersessies die SSH gebruiken, evenals statistiek-verzamelen met SNMP of NetFlow. Wanneer u de beveiliging van een netwerkapparaat in overweging neemt, is het van cruciaal belang dat het beheervlak wordt beschermd. Als een veiligheidsincident de functies van het managementvliegtuig kan ondermijnen, kan het voor u onmogelijk zijn om het netwerk te herstellen of te stabiliseren.

Hardnekkig beheersplan

Het beheersvliegtuig wordt gebruikt om toegang te krijgen tot, te vormen en een apparaat te beheren, evenals zijn operaties en het netwerk te controleren waarop het wordt ingezet. Het beheersvliegtuig is het vliegtuig dat verkeer ontvangt en verstuurt voor de exploitatie van deze functies. Deze lijst van protocollen wordt gebruikt door het managementvlak:

- Eenvoudig netwerkbeheerprotocol
- Secure Shell-protocol
- File Transfer Protocol
- Trial File Transfer Protocol
- Secure-kopiëren
- TACACS+
- RADIUS
- NetFlow
- Netwerktijdprotocol
- Syslog
- ICMP
- MKB

  Opmerking: Het in werking stellen van TELNET wordt niet aanbevolen, aangezien het gewone tekst is.

Wachtwoordbeheer

Wachtwoorden regelen de toegang tot hulpmiddelen en hulpmiddelen. Dit wordt bereikt door de definitie een wachtwoord of geheim dat wordt gebruikt om verzoeken voor authenticatie te verklaren. Wanneer een verzoek om toegang tot een bron of apparaat wordt ontvangen, wordt het verzoek ter verificatie van het wachtwoord en de identiteit betwist, en kan toegang worden verleend, geweigerd of beperkt op basis van het resultaat. Als best practice moeten wachtwoorden worden beheerd met een TACACS+ of RADIUS-verificatieserver. Merk op dat een lokaal ingesteld wachtwoord voor bevoorrechte toegang nog steeds nodig is in geval van een storing van de TACACS+ of RADIUS-diensten. Een apparaat kan ook andere wachtwoordinformatie hebben die binnen zijn configuratie aanwezig is, zoals een NTP-toets, SNMP-community-string of Routing Protocol-toets.

ASA gebruikt Message Digest 5 (MD5) voor het hashen van het wachtwoord. Dit algoritme heeft een aanzienlijke publieke recensie gehad en is waarvan bekend is dat het omkeerbaar is. De algoritme is echter onderworpen aan woordenboekaanvallen. Bij een woordenboekaanval probeert een aanvaller elk woord in een woordenboek of een andere lijst met kandidaat-wachtwoorden om een overeenkomst te vinden. Daarom moeten configuratiebestanden veilig worden opgeslagen en alleen worden gedeeld met vertrouwde individuen.

HTTP-service inschakelen

Om ASDM te gebruiken, moet u de HTTPS server inschakelen en HTTPS verbindingen naar de ASA toestaan. Het security apparaat maakt maximaal 5 gelijktijdige ASDM-exemplaren per context mogelijk, indien beschikbaar, met een maximum van 32 ASDM-exemplaren tussen alle contexten. Zo configureren:

```
http server enable <port>
```

staan alleen de IP toe die in de ACL-lijst nodig zijn. Het toestaan van een brede toegang is een verkeerde praktijk.

```
http 0.0.0.0 0.0.0.0 <interface>
```

ASDM toegangscontrole instellen:

```
http <remote_ip_address> <remote_subnet_mask> <interface_name>
```

Om te beginnen met ASA-softwarerelease 9.1(2),8.4(4.1), ondersteunt de ASA nu de volgende voorlopige DIffie-Hellman (DHE) SSL-algoritmen.

DHE-AES128-SHA1
DHE-AES256-SHA1

Deze algoritme-formaten worden gespecificeerd in **RFC 3268**, Advanced Encryption Standard (AES) Cipherseries voor Transport Layer Security (TLS).

Wanneer ondersteund door de cliënt, is DHE het preferente algoritme omdat het Perfect Forward Secundaire verstrekt. Zie de volgende beperkingen:

DHE wordt niet ondersteund op SSL 3.0 verbindingen, dus zorg ervoor dat u ook TLS 1.0 voor de SSL server inschakelen.

```
// Set server version ASA(config)# ssl server-version tlsv1 sslv3
// Set client version ASA(config) # ssl client-version any
```

Sommige populaire toepassingen ondersteunen DHCP niet, dus omvatten minstens één andere SSL encryptie methode om te verzekeren dat een algoritme die zowel de SSL client als de server gemeenschappelijk heeft kan worden gebruikt. Sommige klanten kunnen geen DHE, waaronder AnyConnect 2.5 en 3.0, Cisco Secure Desktop en Internet Explorer 9.0 ondersteunen.

De ASA heeft onderstaande ciphers in de volgorde ingeschakeld.

```
ASA(config)#ssl encryption rc4-sha1 dhe-aes128-sha1 dhe-aes256-sha1 aes128-sha1 aes256-sha1
3des-sha1
```

SLB: serverversie (standaard)

De ASA gebruikt standaard een tijdelijk zelfgetekend certificaat dat bij elke herstart verandert. Als u op zoek bent naar één certificaat, kunt u de onderstaande link volgen om een permanent zelf-ondertekend certificaat te genereren.

ASA ondersteunt TLS versie 1.2 vanaf softwareversie 9.3.1 voor beveiligde berichtoverdracht voor ASDM, Clientloze VPN en AnyConnect VPN. De volgende opdrachten zijn geïntroduceerd of aangepast: **ssl client-versie**, **ssl server-versie**, **ssl algoritme**, ssl trust-point, **ssl dh-group**, show ssl, show ssl algoritme, show vpn-sessiondb

```
ASA-1/act(config)# ssl server-version ?

configure mode commands/options:
  tlsv1    Enter this keyword to accept SSLv2 ClientHellos and negotiate TLSv1
           (or greater)
  tlsv1.1  Enter this keyword to accept SSLv2 ClientHellos and negotiate
           TLSv1.1 (or greater)
  tlsv1.2  Enter this keyword to accept SSLv2 ClientHellos and negotiate
           TLSv1.2 (or greater)
```

```
ASA-1/act(config)# ssl cipher ?

configure mode commands/options:
  default  Specify the set of ciphers for outbound connections
  dtlsv1   Specify the ciphers for DTLSv1 inbound connections
  tlsv1    Specify the ciphers for TLSv1 inbound connections
  tlsv1.1  Specify the ciphers for TLSv1.1 inbound connections
  tlsv1.2  Specify the ciphers for TLSv1.2 inbound connections
```

SSH inschakelen

De ASA staat SSH-verbindingen met de ASA toe voor beheerdoeleinden. ASA staat een maximum van 5 gelijktijdige SSH-verbindingen per context toe, indien beschikbaar, met een maximum van 100 verbindingen verdeeld over alle contexten.

```
hostname <device_hostname>
domain-name <domain-name>
crypto key generate rsa modulus 2048
```

Het standaard sleutelpaar is een algemene toets. De standaard modulusgrootte is 1024. De hoeveelheid NVRAM ruimte voor het opslaan van sleutelparen varieert afhankelijk van het ASA platform. U kunt een limiet bereiken als u meer dan 30 sleutelparen genereert. De 4096-bits RSA-toetsen worden alleen ondersteund op de ASA 5580, 5585 of later platforms.

Zo verwijdert u de sleutelparen van het aangegeven type (rsa of dsa)

```
crypto key zeroize { rsa | dsa } [ label key-pair-label ] [ default ] [ noconfirm ]
```

SSH configureren voor toegang externe apparaat:

```
ssh <remote_ip_address> <remote_subnet_mask> <interface_name>
```

Om de versie van SSH die door de ASA is geaccepteerd te beperken, gebruikt u de ssh versie-opdracht in de mondiale configuratiemodus. ASA beperken om alleen versie 2 te gebruiken kan onder opdracht worden uitgevoerd.

```
ASA(config)#ssh version 2
```

Om sleutels te ruilen met behulp van of de Diffie-Hellman (DH) Group 1 of DH Group 14 key exchange methode, gebruik dan de ssh key-exchange opdracht in globale configuratie modus. met ingang van 9.1(2) ASA ondersteunt dh-groep14-sha1 voor SSH

```
ASA(config)#ssh key-exchange dh-group14-sha1
```

Time-out instellen voor inlogsessies

```
// Configure Console timeout
ASA(config)#console timeout 10

// Configure Console timeout
ASA(config)#ssh timeout 10
```

Wachtwoordbeheer

Wachtwoorden regelen de toegang tot hulpmiddelen en hulpmiddelen. Dit wordt bereikt door de definitie een wachtwoord of geheim dat wordt gebruikt om verzoeken voor authenticatie te verklaren. Wanneer een verzoek om toegang tot een bron of apparaat wordt ontvangen, wordt het verzoek ter verificatie van het wachtwoord en de identiteit betwist, en kan toegang worden verleend, geweigerd of beperkt op basis van het resultaat. Als best practice moeten wachtwoorden worden beheerd met een TACACS+ of RADIUS-verificatieserver. Merk op dat een lokaal ingesteld wachtwoord voor bevoorrechte toegang nog steeds nodig is in geval van een storing van de TACACS+ of RADIUS-diensten. Een apparaat kan ook andere wachtwoordinformatie hebben die binnen zijn configuratie aanwezig is, zoals een NTP-toets, SNMP-community-string of Routing Protocol-toets.

Local User en Encrypt Password configureren

```
username <local_username> password <local_password> encrypted
```

Wachtwoord instellen

```
enable password <enable_password> encrypted
```

AAA-verificatie configureren voor modus inschakelen

```
ASA(config)#aaa authentication enable console LOCAL
```

Verificatie, autorisatie en accounting

Het kader voor verificatie, autorisatie en accounting (AAA) is cruciaal om interactieve toegang tot netwerkapparaten te garanderen. Het AAA-kader biedt een zeer aanpasbare omgeving die op basis van de behoeften van het netwerk kan worden aangepast.

TACACS+ verificatie

TACACS+ is een authenticatieprotocol dat ASA kan gebruiken voor verificatie van beheergebruikers tegen een externe AAA-server. Deze beheergebruikers kunnen het ASA-apparaat benaderen via SSH, HTTPS, telnet of HTTP.

TACACS+-verificatie, of meer in het algemeen AAA-verificatie, biedt de mogelijkheid om voor elke netwerkbeheerder individuele gebruikersrekeningen te gebruiken. Als u niet afhankelijk bent van één gedeeld wachtwoord, wordt de beveiliging van het netwerk verbeterd en wordt uw verantwoordingsplicht versterkt.

RADIUS is een protocol dat vergelijkbaar is met TACACS+; het versleutelt echter alleen het wachtwoord dat over het netwerk wordt verzonden. In contrast hiermee versleutelt TACACS+ de gehele TCP-lading, die zowel de gebruikersnaam als het wachtwoord bevat. Om deze reden zou TACACS+ in plaats van RADIUS moeten worden gebruikt wanneer TACACS+ door de AAA server wordt ondersteund. Raadpleeg TACACS+ en RADIUS-vergelijking voor een gedetailleerdere vergelijking van deze twee protocollen.

De verificatie van TACACS+ kan worden ingeschakeld op een Cisco ASA-apparaat met een configuratie vergelijkbaar met dit voorbeeld:

```
aaa authentication serial console Tacacs
aaa authentication ssh console Tacacs
aaa authentication http console Tacacs
aaa authentication telnet console Tacacs
```

ASA-ondertekening en verificatie van beelden

Vanaf softwareversie 9.3.1 ASA-beelden worden nu ondertekend met een digitale handtekening. De digitale handtekening wordt geverifieerd nadat de ASA is gestart.

```
ASA-1/act(config)# verify flash:/asa941-smp-k8.bin
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!Done! Embedded Hash SHA-512:
0e707a0e45b1c7c5afa9ef4e802a273677a5e46f7e1d186292abe1154
c948a63c625463b74119194da029655487659490c2873506974cab78b66d6d9742ed73e Computed Hash SHA-512:
0e707a0e45b1c7c5afa9ef4e802a273677a5e46f7e1d186292abe1154
c948a63c625463b74119194da029655487659490c2873506974cab78b66d6d9742ed73e CCO Hash SHA-512:
1b6d41e893868aab9e06e78a9902b925227c82d8e31978ff2c412c18a
c99f49f70354715441385e0b96e4bd3e861d18fb30433d52e12b15b501fa790f36d0ea0 Signature Verified
ASA(config)# verify /signature running Requesting verify signature of the running image...
Starting image verification Hash Computation: 100% Done! Computed Hash SHA2:
2fbb0f62b5fbc61b081acfca76bddbb2 26ce7a5fb4b424e5e21636c6c8a7d665
1e688834203dfb7ffa6eaefc7fdf9d3d 1d0a063a20539baba72c2526ca37771c Get key records from key
storage: PrimaryASA, key_store_type: 6 Embedded Hash SHA2: 2fbb0f62b5fbc61b081acfca76bddbb2
26ce7a5fb4b424e5e21636c6c8a7d665 1e688834203dfb7ffa6eaefc7fdf9d3d
1d0a063a20539baba72c2526ca37771c Returned. rc: 0, status: 1 The digital signature of the running
image verified successfully

ASA-1/act(config)# show software authenticity running
Image type : Release
Signer Information
Common Name : abraxas
Organization Unit : ASAv
Organization Name : CiscoSystems
Certificate Serial Number : 550DBBD5
Hash Algorithm : SHA2 512
Signature Algorithm : 2048-bit RSA
Key Version : A
```

Kloktijd instellen

```
clock timezone GMT <hours offset>
```

NTP configureren

Het Network Time Protocol (NTP) is geen bijzonder gevaarlijke service, maar elke overbodige service kan een aanvalsvector vertegenwoordigen. Als NTP wordt gebruikt, is het belangrijk om expliciet een vertrouwde tijdbron te configureren en juiste authenticatie te gebruiken. Nauwkeurige en betrouwbare tijd is vereist voor syslig-doeleinden, zoals tijdens forensisch onderzoek van mogelijke aanvallen, en voor succesvolle VPN-connectiviteit wanneer dit afhankelijk is van certificaten voor Fase 1-verificatie.

- **NTP Time Zone** - Wanneer u NTP configureren moet de tijdzone worden ingesteld zodat tijdstempels accuraat gecorreleerd kunnen worden. Er zijn gewoonlijk twee benaderingen om de tijdzone voor apparaten in een netwerk met een mondiale aanwezigheid te vormen. Eén methode is om alle netwerkapparaten aan te passen met de gecoördineerde Universal Time (UTC) (voorheen Greenwich Mean Time (GMT)). De andere benadering is om netwerkapparaten met de lokale tijdzone te configureren.

```
ntp server ip_address [ key key_id ] [ source interface_name ] [ prefer ]
```

- **NTP-verificatie** - Als u de NTP-verificatie configureren biedt deze de garantie dat NTP-berichten worden uitgewisseld tussen vertrouwde NTP-peers. Verificatie inschakelen met de opdracht NTP-authenticatie, stelt de vertrouwde sleutel-ID in voor deze server. Als u authenticatie toelaat, communiceert de ASA slechts met een NTP server als het de juiste vertrouwde sleutel in de pakketten gebruikt. Om authenticatie met een NTP server mogelijk te maken, gebruik de ntp authenticate opdracht in mondiale configuratiewijze.

```
ASA(config)#ntp authenticate
```

DHCP-serverservice (indien niet gebruikt)

```
clear configure dhcpd
no dhcpd enable <interface_name>
```

Opmerking: ASA ondersteunt CDP niet.

Toegangslijst van besturingsplane

Toegangscontroleregels voor aan-de-box beheersverkeer (gedefinieerd door opdrachten als http, ssh of telnet) hebben een hogere voorrang dan een toegangslijst die wordt toegepast met de optie besturingsplane. Daarom zal een dergelijk toegestaan beheerverkeer ook mogen worden binnengebracht indien het uitdrukkelijk wordt ontkend door de toegangslijst voor het gebruik van een doos.

```
access-list <name> in interface <Interface_name> control-plane
```

Van ASA

Dit zijn de protocollen die kunnen worden gebruikt om bestanden naar ASA te kopiëren/over te

dragen.

Tekst wissen:

- FTP
- HTTP
- TFTP
- MKB

Beveiliging:

- HTTPS
- SCP (Secure Copy Client) vanaf 9.1(5) ondersteunt ASA SCP client om bestanden naar en van een SCP server over te brengen.

Voor doorgaand verkeer

TCP-sequentie-randomisatie

Elke TCP-verbinding heeft twee ISN's: een door de client gegenereerd en een door de server gegenereerd. De ASA regelt de ISDN van het TCP SYN dat zowel de inkomende als de uitgaande kant passeert.

Randomiseren met ISN van de beschermde gastheer voorkomt een aanvaller van tevoren de volgende ISDN voor een nieuwe verbinding en kaping van de nieuwe sessie.

Indien nodig kan de randomisatie van TCP-beginsequentienummer worden uitgeschakeld. Bijvoorbeeld:

- Als een andere inline firewall ook de aanvankelijke opeenvolgingsnummers willekeurig maakt, hoeven beide firewalls deze actie niet uit te voeren, ook al heeft deze actie geen invloed op het verkeer.
- Als u eBGP multi-hop via de ASA gebruikt, en de eBGP peers gebruiken MD5. Randomisatie breekt de MD5 checksum.
- Als we een WAAS-apparaat gebruiken dat van de ASA eist dat hij de sequentienummers van verbindingen niet willekeurig maakt.

TTL-decrement

Standaard wordt TTL in de IP-header niet verlaagd, waarbij ASA niet als router-hop verschijnt bij het doen van Traceroute.

dansbewaker

Voert één DNS-respons per query in. U kunt deze functie inschakelen door de opdracht in de mondiale configuratiemodus te gebruiken.

```
ASA(config)#dns-guard
```

Controles van fragmentatieketen configureren

Om extra beheer van pakketfragmentatie te bieden en compatibiliteit met NFS te verbeteren, gebruikt u de fragment-opdracht in de mondiale configuratiemodus.

```
fragment reassembly { full | virtual } { size | chain | timeout limit } [ interface ]
```

Protocolinspectie configureren

Inspectiemachines zijn vereist voor diensten die IP-adresinformatie insluiten in het gebruikerspakket of die secundaire kanalen openen op dynamisch toegewezen poorten. Deze protocollen vereisen dat de ASA een diepe pakketinspectie uitvoert in plaats van het pakket door het snelle pad te geven. Als gevolg daarvan kunnen inspectiemachines de totale doorvoersnelheid beïnvloeden. Raadpleeg ASA 9.4 Config-handleiding voor meer informatie over Application Layer Protocol-inspectie.

Inspectie op ASA kan worden ingeschakeld met behulp van onderstaande opdracht

```
policy-map <Policy-map_name>
 class inspection_default
  inspect <Protocol>

service-policy <Policy-map_name> interface <Interface_name> (Per Interface)
service-policy <Policy-map_name> global (Globally)
```

Standaard heeft ASA **"global_policy"** mondiaal ingeschakeld.

Unicast omgekeerd pad doorsturen

```
ip verify reverse-path interface <interface_name>
```

Wanneer het verkeer achteruit gaat als gevolg van de controle van RPF, de onderstaande "show asp drop" teller in ASA stappen.

```
ASA(config)# show asp drop

Frame drop:
 Invalid TCP Length (invalid-tcp-hdr-length)                 21

  Reverse-path verify failed (rpf-violated)                   90

// Check Reverse path statistics

ASA(config)# sh ip verify statistics

interface inside: 11 unicast rpf drops
```

interface outside: 79 unicast rpf drops

Detectie van bedreigingen

Threat Detectie biedt firewallbeheerders met de benodigde gereedschappen om aanvallen te identificeren, te begrijpen en te stoppen voordat ze de interne netwerkinfrastructuur bereiken. Om dit te doen, is de functie gebaseerd op een aantal verschillende triggers en statistieken, die in deze paragrafen nader worden beschreven.

Raadpleeg de ASA-functie voor detectie van bedreigingen en configuratie voor meer informatie over detectie van bedreigingen bij ASA.

Botfilter

Het BotNet-verkeersfilter controleert verzoeken en reacties van Domain Name Server (DNS) tussen interne DNS-clients en externe DNS-servers. Wanneer een DNS-respons wordt verwerkt, wordt het domein dat met de respons wordt geassocieerd, gecontroleerd aan de hand van de database met bekende kwaadaardige domeinen. Als er een match is, wordt al het verdere verkeer naar het IP-adres dat in de DNS-respons aanwezig is geblokkeerd.

Malware is kwaadaardige software die op een onbekende host is geïnstalleerd. Malware die netwerkactiviteit probeert te verzenden zoals privé gegevens (wachtwoorden, creditcardnummers, toetsenstrepen of eigen gegevens) kan door het Botnet Traffic Filter worden gedetecteerd wanneer de malware een verbinding met een bekend slecht IP-adres start. Het Botnet Traffic Filter controleert inkomende en uitgaande verbindingen met een dynamische database met bekende slechte domeinnamen en IP-adressen (de *zwarte lijst*), en logt dan elke verdachte activiteit in of blokkeert deze.

U kunt de Cisco dynamische database ook aanvullen met adressen van uw keuze door ze aan een statische zwarte lijst toe te voegen. als de dynamische database adressen bevat die volgens u niet op de zwarte lijst moeten staan , kunt u ze handmatig in een statische *witlijst* invoeren . Whitelisted-adressen genereren nog steeds syslog-berichten, maar omdat je alleen zwartlijstboodschappen richt, zijn ze informatief. Zie Het netto-verkeersfilter configureren voor meer informatie.

ARP cache-toevoegingen voor niet-aangesloten subnetten

Standaard zal ASA niet reageren op ARP voor niet-direct verbonden IP-adressen. Als u een NAT IP op ASA hebt die niet tot zelfde netwerk IP van de ASA interface behoort, zullen wij "arp vergunning-niet-verbonden" op ASA aan proxy-ARP voor NATted IP moeten toelaten.

```
arp permit-nonconnected
```

Het wordt altijd aanbevolen om de juiste routing op stroomopwaarts en stroomafwaarts gerichte apparatuur te hebben zodat NAT kan werken zonder de bovenstaande opdracht toe te staan.

Vastlegging en bewaking

SNMP configureren

In deze sectie worden een aantal methoden beschreven die kunnen worden gebruikt om de implementatie van SNMP binnen ASA-apparaten te beveiligen. Het is van cruciaal belang dat SNMP correct wordt beveiligd om de vertrouwelijkheid, integriteit en beschikbaarheid van zowel de netwerkgegevens als de netwerkapparaten te beschermen waardoor deze gegevens worden doorgegeven. SNMP biedt u een schat aan informatie over de gezondheid van netwerkapparaten. Deze informatie moet worden beschermd tegen kwaadwillige gebruikers die deze gegevens willen gebruiken om aanvallen tegen het netwerk uit te voeren.

SNMP-community-Streng

Community strings zijn wachtwoorden die worden toegepast op een ASA apparaat om de toegang tot de SNMP-gegevens op het apparaat te beperken, zowel read-only als read-Writing. Deze community strings moeten, net als alle wachtwoorden, zorgvuldig worden gekozen om er zeker van te zijn dat ze niet triviaal zijn. De communautaire koorden moeten op gezette tijden en in overeenstemming met het beveiligingsbeleid van het netwerk worden gewijzigd. Bijvoorbeeld, zouden de koorden moeten worden veranderd wanneer een netwerkbeheerder rollen verandert of het bedrijf verlaat.

SNMP-leestoegang inschakelen:

```
snmp-server host <interface_name> <remote_ip_address>
```

SNMP-trap inschakelen

```
snmp-server enable traps all
```

Syslog configureren

Het wordt geadviseerd om loginformatie naar een afstandsbediening te sturen. Dit maakt het mogelijk om netwerk- en beveiligingsgebeurtenissen over netwerkapparaten effectiever te correleren en te controleren. Merk op dat syslogberichten onbetrouwbaar worden verzonden door UDP en in cleartext. Om deze reden moet elke bescherming die een netwerk biedt aan beheerverkeer (bijvoorbeeld encryptie of toegang buiten de band) worden uitgebreid, zodat het ook systeemverkeer omvat. Logs kunnen worden gebruikt om vanuit ASA naar de volgende bestemming te worden verstuurd:

- ASDM
- buffer
- Flitser
- Email
- FTP-server
- SNMP-server als vallen
- Syslogserver

Logernst van console configureren

```
logging console critical
```

TCP-gebaseerde syslog is ook beschikbaar. Alle syslogs kunnen worden verzonden naar de syslogserver in plaats van in gecodeerde vorm of in geval van TCP.

Plaintext

logging interface_name syslog_ip [tcp / poort

Versleuteld

logging host *interface_name syslog_ip* [**tcp/**poort / [**veilig**]

Als een TCP-verbinding niet met de Slogs server tot stand kan worden gebracht, worden alle nieuwe verbindingen ontkend. U kunt dit standaardgedrag wijzigen door de opdracht "**houtkap" in** te voeren.

Tijdlijnen in logberichten configureren

De configuratie van loggtimestamps helpt u gebeurtenissen over netwerkapparaten te correleren. Het is belangrijk om een correcte en consistente configuratie van de logtijd uit te voeren om ervoor te zorgen dat u de loggegevens kunt correleren.

```
logging timestamp
```

Raadpleeg voor aanvullende informatie over syslog het voorbeeld ASA SLOG Configuration.

NetFlow configureren

Soms moet u netwerkverkeer snel identificeren en traceren, vooral tijdens de respons van het incident of slechte netwerkprestaties. NetFlow kan zicht bieden in al het verkeer op het netwerk. Daarnaast kan NetFlow worden geïmplementeerd met verzamelaars die lange termijn trending en geautomatiseerde analyse kunnen bieden.

Cisco ASA ondersteunt NetFlow versie 9-services. De ASA en ASASASM implementaties van NSEL bieden een stateful, IP flow tracking methode die alleen die records exporteert die significante gebeurtenissen in een flow aangeven. Bij stateful flow tracking gaan de getraceerde stromen door een reeks veranderingen van de staat. NSEL gebeurtenissen worden gebruikt om gegevens over flow status te exporteren en worden geactiveerd door de gebeurtenis die de verandering van de staat veroorzaakte.

Raadpleeg Cisco ASA NetFlow Implementatie Guide voor meer informatie over NetFlow op ASA:

Beveiligende configuratie

Beeldverificatie op ASA

Vanaf 9.1(2) en 8.4(4.1) werd ondersteuning voor de controle op de beeldintegriteit van SHA-512 toegevoegd. Om de checksum van een bestand te verifiëren, gebruik de verify-opdracht in geprivilegieerde EXEC-modus.

Berekent en geeft de MD5 waarde voor het gespecificeerde softwarebeeld weer. Vergelijk deze waarde met de waarde die op Cisco.com beschikbaar is voor deze afbeelding.

```
verify [ /md5 path ] [ md5-value ]
```

Wachtwoorden in de configuratie

Alle wachtwoorden en de toetsen worden versleuteld of verduisterd. De "show in werking stellen-configuratie" ontheft niet de eigenlijke wachtwoorden.

Een dergelijke back-up kan niet worden gebruikt voor back-up/herstel op ASA. De back-up die wordt genomen voor terugzetdoeleinden moet worden uitgevoerd met behulp van de opdracht "meer systeem:in werking stellen-configuratie".De wachtwoorden van de ASA-configuratie kunnen worden versleuteld met een master pass-zin. Raadpleeg de wachtwoordencryptie voor meer informatie.

Terugwinning van servicewachtwoord

Door dit uit te schakelen wordt het wachtwoordterugwinningsmechanisme uitgeschakeld en wordt de toegang tot ROMMON uitgeschakeld. De enige manier om verloren of vergeten wachtwoorden te herstellen is voor ROMMON om alle bestandssystemen, inclusief configuratiebestanden en afbeeldingen, te wissen. U dient een back-up van de configuratie te maken en een mechanisme te hebben om afbeeldingen uit de opdrachtregel van ROMMON te herstellen.

Problemen oplossen

Er is geen sectie voor probleemoplossing voor dit document.