ASA/PIX 7.x en later: De netwerkaanvallen beperken

Inhoud

Inleiding

Dit document beschrijft hoe de verschillende netwerkaanvallen, zoals Denial-of-Services (DoS), kunnen worden beperkt met behulp van Cisco Security Appliance (ASA/PIX).

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco 5500 Series adaptieve security applicatie (ASA) die softwareversie 7.0 en hoger uitvoert.

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

Dit document kan ook worden gebruikt met Cisco 500 Series PIX die softwareversie 7.0 en hoger uitvoeren.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Beveiliging tegen SYN-aanvallen

Hoe milder u de TCP- (Transmission Control Protocol) synchroniseer/start-aanvallen (SYN) op de ASA/PIX?

TCP SYN-aanval

TCP SYN-aanval is een type DoS-aanval waarbij een zender een volume verbindingen doorgeeft dat niet kan worden voltooid. Dit veroorzaakt dat de verbindingsrijen worden vuld, waarbij de dienst aan legitieme TCP gebruikers wordt ontkend.

Wanneer een normale TCP verbinding start, ontvangt een doelhost een SYN-pakket van een bronhost en stuurt u een synchrone erkennen (SYN ACK) terug. De doelhost moet dan een ACK van de SYN ACK horen voordat de verbinding wordt ingesteld. Dit wordt de TCP-drievoudige handdruk genoemd.

Terwijl het wachten op ACK aan SYN ACK, houdt een verbindingsrij van eindige grootte op de bestemmingshost bij het wachten op voltooiing van de verbindingen. Deze rij leegt gewoonlijk snel omdat de ACK een paar milliseconden na de SYN ACK verwacht wordt.

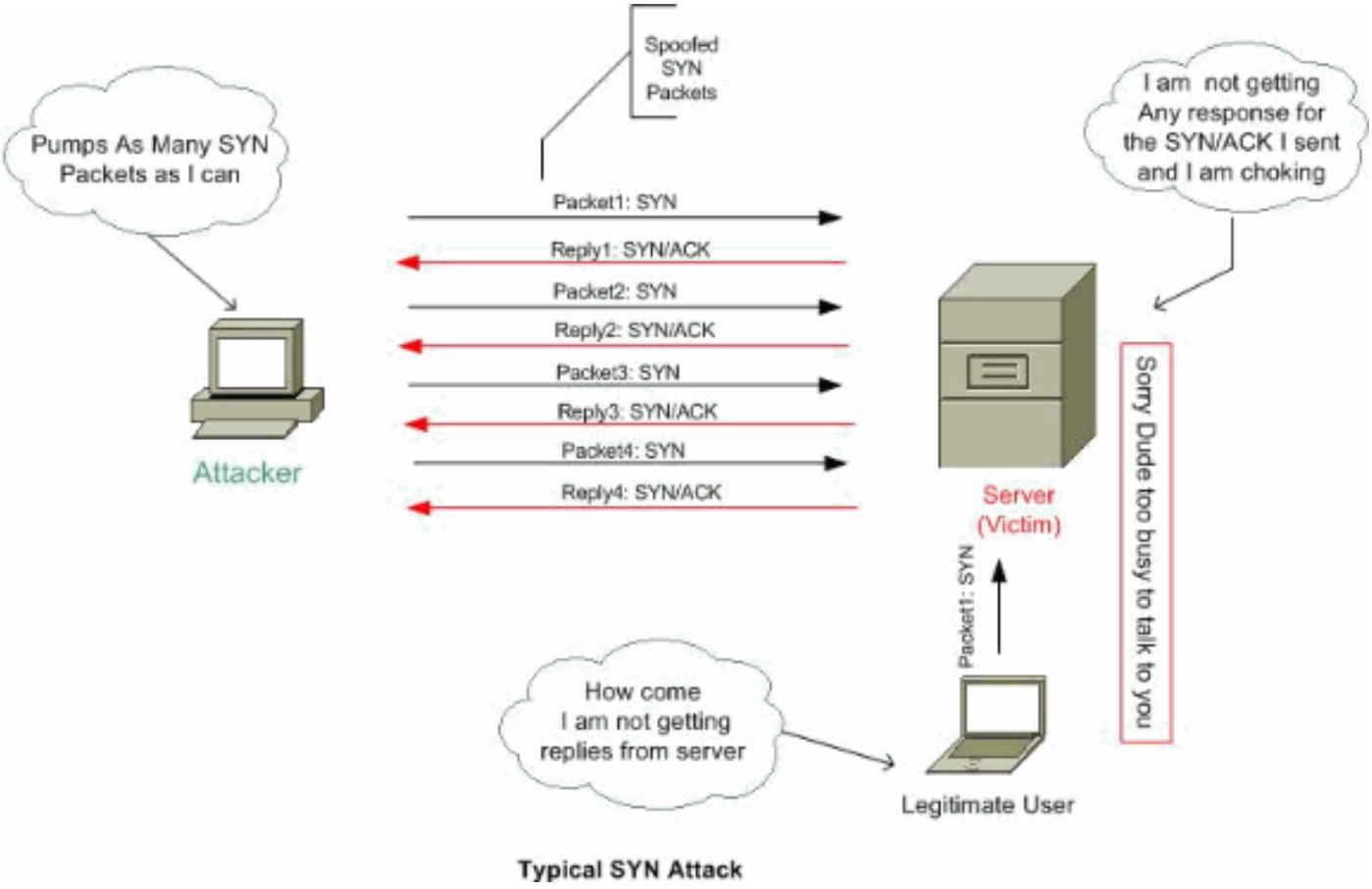
De TCP SYN-aanval buit dit ontwerp door een aanvallende bronhost te hebben die TCP SYN-pakketten met willekeurige bronadressen naar een slachtoffer-host genereren. De gastheer van de slachtoffer bestemming stuurt een SYN ACK terug naar het willekeurige bronadres en voegt een ingang aan de verbindingsrij toe. Omdat de SYN ACK voor een onjuiste of niet bestaande gastheer bestemd is, wordt het laatste deel van de "drierichtings handdruk" nooit voltooid en de ingang in de verbindingsrij blijft tot een timer afloopt, gewoonlijk ongeveer een minuut. Door enige TCP SYN-pakketten te genereren uit willekeurige IP-adressen met een hoge snelheid, is het mogelijk de verbindingswachtrij te vullen en de TCP-services (zoals e-mail, bestandsoverdracht of WWW) aan legitieme gebruikers te ontkennen.

Er is geen makkelijke manier om de originator van de aanval te vinden omdat het IP-adres van de bron vervalst is.

De externe manifestaties van het probleem omvatten het onvermogen om e-mail te krijgen, het onvermogen om verbindingen met WW of FTP services te accepteren of een groot aantal TCP verbindingen op uw host in de staat SYN_RCVD.

Raadpleeg Defensie tegen TCP SYN-overstromingen voor meer informatie over TCP SYN-

aanvallen.



Typical SYN Attack

Beperken

In deze sectie wordt beschreven hoe de SYN-aanvallen kunnen worden verzacht door de maximale TCP- en User Datagram Protocol (UDP)-verbindingen, de maximale embryonale verbindingen, de aansluitingstijd en de manier waarop u de randomisatie van de TCP-sequentie kunt uitschakelen.

Als de embryonale verbindingsgrens wordt bereikt, reageert het veiligheidsapparaat op elk SYN-pakket dat naar de server wordt verzonden met een SYN+ACK en gaat het SYN-pakket niet naar de interne server. Als het externe apparaat reageert met een ACK-pakket, dan weet het beveiligingsapparaat dat het een geldig verzoek is (en geen deel uitmaakt van een potentiële SYN-aanval). Het beveiligingsapparaat maakt vervolgens een verbinding met de server en sluit zich aan bij de verbindingen. Als het beveiligingsapparaat geen ACK terug krijgt van de server, dan wordt de embryonale verbinding agressief uitgesteld.

Elke TCP-verbinding heeft twee Initiële reeks Number (ISN's): een door de client gegenereerd en een door de server gegenereerd. Het veiligheidsapparaat randomiseert ISDN van het TCP SYN dat in zowel de inkomende als de uitgaande richtingen passeert.

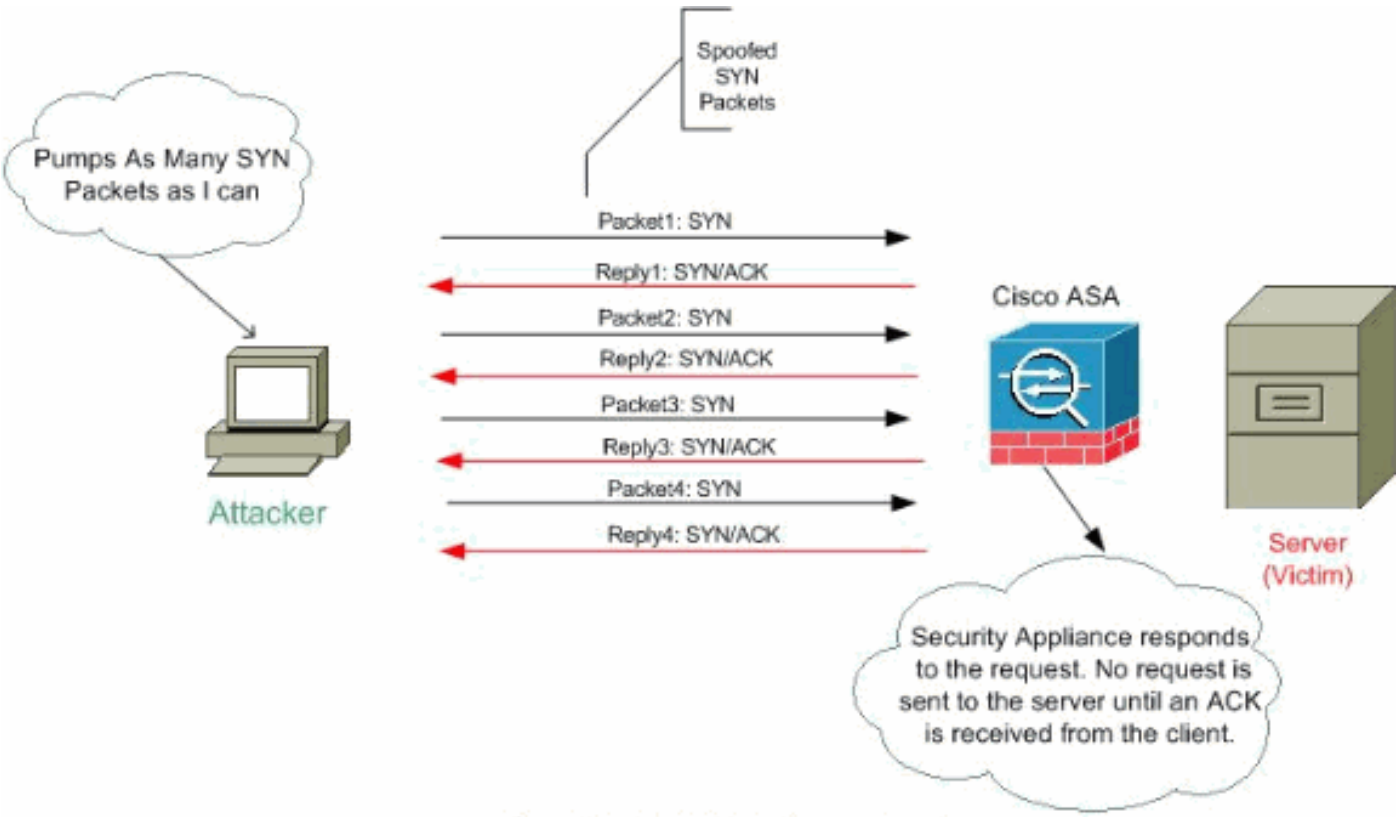
Randomisatie op ISDN van de beschermde gastheer voorkomt een aanvaller van het voorspellen van de volgende ISDN voor een nieuwe verbinding en het kapen van de nieuwe sessie.

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 externe BGP (eBGP) meerdere hop via het security apparaat gebruikt, en de eBGP-peers gebruik maken van MD5, breekt randomisatie de MD5 checksum uit.
- U gebruikt een WAAS-apparaat (Wide Area Application Services) dat van het security apparaat vereist dat u de sequentienummers van de verbindingen niet willekeurig selecteert.

Opmerking: U kunt ook maximale connecties, maximale embryonale verbindingen en TCP sequentie randomisatie in de NAT configuratie configureren. Als u deze instellingen voor hetzelfde verkeer instelt op basis van beide methoden, gebruikt het security apparaat de onderste limiet. Voor randomisatie van de TCP-sequentie, als het wordt uitgeschakeld met behulp van een van beide methoden, schakelt het security apparaat de TCP-sequentie-randomisatie uit.



Security Appliance acts as a proxy

Volg deze stappen om de verbindingsgrenzen in te stellen:

1. Om het verkeer te identificeren, voeg een class map toe met de **class-map** opdracht volgens het modulaire beleidskader.
2. Als u een **beleidskaart** wilt toevoegen of bewerken die de acties instelt die u met het class map traffic wilt uitvoeren, voert u deze opdracht in:
   ```
   hostname(config)#policy-map name
   ```
3. Om de class map (uit stap 1) te identificeren waaraan u een actie wilt toewijzen, voert u deze opdracht in:
   ```
   hostname(config-pmap)#class class_map_name
   ```
4. Om de maximum connecties (zowel TCP als UDP) in te stellen, treden de maximum embryonale verbindingen, per-client-embryonaal-max, per-client-max of om TCP-sequentirandomisatie uit te schakelen deze opdracht in:
   ```
   hostname(config-pmap-c)#set connection {[conn-max number]
   [embryonic-conn-max number] [per-client-embryonic-max number]
   ```

```
[per-client-max number][random-sequence-number {enable |
disable}}
```

Waar number een integer is tussen 0 en 65535. De default is 0, wat betekent geen limiet op verbindingen.U kunt deze opdracht allemaal op één regel invoeren (in elke volgorde), of u kunt elke eigenschap als een afzonderlijke opdracht invoeren. De opdracht wordt in de actieve configuratie op één regel gecombineerd.

5. Om de tijd voor connecties, embryonale verbindingen (half geopend) en half gesloten verbindingen in te stellen, voer deze opdracht in:

```
hostname(config-pmap-c)#set connection {[embryonic hh[:mm[:ss]]]
[half-closed hh[:mm[:ss]]] [tcp hh[:mm[:ss]]]}
```

Waar **embryonaal** hh[:mm[:ss] een tijd is tussen 0:0:5 en 1192:59:59. De standaard is 0:0:30. Je kunt deze waarde ook instellen op 0, wat betekent dat de verbinding nooit uitkomt.De **half-gesloten** hh[:mm[:ss] en **tcp** hh[:mm[:ss] waarden zijn een tijd tussen 0:5:0 en 1192:59:59. De standaard voor **half-gesloten** waarden is 0:10:0 en de standaard voor **tcp** is 1:0. kan deze waarden ook op 0 instellen, wat betekent dat de verbinding nooit uitkomt.U kunt deze opdracht allemaal op één regel invoeren (in elke volgorde), of u kunt elke eigenschap als een afzonderlijke opdracht invoeren. De opdracht wordt in de actieve configuratie op één regel gecombineerd.**Embryonische (Half-Open) verbinding**-Een embryonale verbinding is een TCP-verbindingsverzoek dat niet de noodzakelijke handdruk tussen bron en bestemming heeft voltooid.**Half-gesloten verbinding**-half gesloten verbinding is wanneer de verbinding slechts in één richting gesloten is door FIN te verzenden. Echter, TCP sessie wordt nog steeds door peer onderhouden.**Per-client-embryonaal-max**-Het maximum aantal gelijktijdige embryonale verbindingen toegestaan per cliënt, tussen 0 en 65535. Het standaard is 0, wat onbeperkte verbindingen toestaat.**Per-client-max**-Het maximum aantal toegestane gelijktijdige verbindingen per client, tussen 0 en 65535. De standaard is 0, wat onbeperkte verbindingen toestaat.

6. Voer deze opdracht in om de beleidskaart op een of meer interfaces te activeren:

```
hostname(config)#service-policy policymap_name {global | interface interface_name}
```

Waar de **globale** beleidskaart op alle interfaces van toepassing is, en de **interface** past het beleid op één interface toe. Er is slechts één algemeen beleid toegestaan. Je kunt het mondiale beleid omzeilen op een interface door een dienstenbeleid op die interface toe te passen. U kunt slechts één beleidskaart op elke interface toepassen.

Voorbeeld:

```
ciscoasa(config)#class-map tcp_syn
ciscoasa(config-cmap)#match port tcp eq 80
ciscoasa(config-cmap)#exit
ciscoasa(config)#policy-map tcpmap
ciscoasa(config-pmap)#class tcp_syn
ciscoasa(config-pmap-c)#set connection conn-max 100
ciscoasa(config-pmap-c)#set connection embryonic-conn-max 200
ciscoasa(config-pmap-c)#set connection per-client-embryonic-max 10
ciscoasa(config-pmap-c)#set connection per-client-max 5
ciscoasa(config-pmap-c)#set connection random-sequence-number enable
ciscoasa(config-pmap-c)#set connection timeout embryonic 0:0:45
ciscoasa(config-pmap-c)#set connection timeout half-closed 0:25:0
ciscoasa(config-pmap-c)#set connection timeout tcp 2:0:0
ciscoasa(config-pmap-c)#exit
ciscoasa(config-pmap)#exit
ciscoasa(config)#service-policy tcpmap global
```

Opmerking: Gebruik deze opdracht om het totale aantal halfopen sessies voor een bepaalde host te controleren:

```
ASA-5510-8x# show local-host all

Interface dmz: 0 active, 0 maximum active, 0 denied
Interface management: 0 active, 0 maximum active, 0 denied
Interface xx: 0 active, 0 maximum active, 0 denied
Interface inside: 7 active, 18 maximum active, 0 denied

local host: <10.78.167.69>,

    TCP flow count/limit = 2/unlimited

    TCP embryonic count to host = 0

    TCP intercept watermark = unlimited

    UDP flow count/limit = 0/unlimited
```

Opmerking: de lijn, de `TCP embryonale telling aan host`, toont het aantal halfopen sessies.

Beveiliging tegen IP-telefoons

Kan de PIX/ASA IP-nep aanvallen blokkeren?

IP-pakketten

Om toegang te krijgen, creëren Inbrekers pakketten met spoofed bron IP adressen. Dit maakt gebruik van toepassingen die op IP-adressen gebaseerde verificatie gebruiken en leidt tot onbevoegde gebruikers en mogelijk worteltoegang op het doelsysteem. Voorbeelden hiervan zijn rsh en rlogin services.

Het is mogelijk om pakketten door filter-router firewalls te leiden als ze niet zijn ingesteld op filter van inkomende pakketten waarvan het bronadres in het lokale domein is. Het is belangrijk om op te merken dat de beschreven aanval mogelijk is, zelfs wanneer geen antwoordpakketten de aanvaller kunnen bereiken.

Voorbeelden van mogelijke kwetsbare configuraties zijn:

- Proxy-firewalls waarin de proxy-toepassingen het IP-bronadres voor verificatie gebruiken
- Routers naar externe netwerken die meerdere interne interfaces ondersteunen
- Routers met twee interfaces die subneting op het interne netwerk ondersteunen

Beperken

Unicast Reverse Path Forwarding (uRPF) tegen IP-spoofing (een pakket gebruikt een onjuist bron-IP-adres om de ware bron te ontdekken) door ervoor te zorgen dat alle pakketten een bron-IP-adres hebben dat overeenkomt met de juiste bron-interface volgens de routingtabel.

Normaal gezien bekijkt het security apparaat alleen het doeladres wanneer u bepaalt waar u het pakket wilt doorsturen. Unicast RPF geeft het security apparaat op om ook het bronadres te bekijken. Dit is de reden dat het **Omgekeerd Pad Doorsturen** wordt genoemd. Voor elk verkeer dat

u via het security apparaat wilt toestaan, moet de tabel met routing van het security apparaat een route naar het bronadres bevatten. Zie RFC 2267 voor meer informatie.

Opmerking: de `:- %PIX-1-106021: Deny protocol reverse path check van src_addr tot dest_addr op interface int_name` logbericht kan worden gezien wanneer de reverse path check is ingeschakeld. Schakel de reverse path-controle uit met de opdracht **geen IP verify-interface (interfacenaam)** om dit probleem op te lossen:

`no ip verify reverse-path interface (interface name)`

Voor buitenverkeer kan het beveiligingsapparaat bijvoorbeeld de standaardroute gebruiken om aan de Unicast RPF-bescherming te voldoen. Als het verkeer vanuit een externe interface binnenkomt en het bronadres niet bekend is aan de routingtabel, gebruikt het security apparaat de standaardroute om de externe interface correct als de broninterface te identificeren.

Als het verkeer de externe interface invoert vanaf een adres dat bekend is aan de routingtabel, maar gekoppeld is aan de interne interface, dan laat het beveiligingsapparaat het pakket vallen. Op dezelfde manier laat het security apparaat, als er verkeer de interne interface via een onbekend bronadres binnenkomt, het pakket vallen omdat de bijbehorende route (de standaardroute) de externe interface aangeeft.

Unicast RPF wordt uitgevoerd zoals wordt getoond:

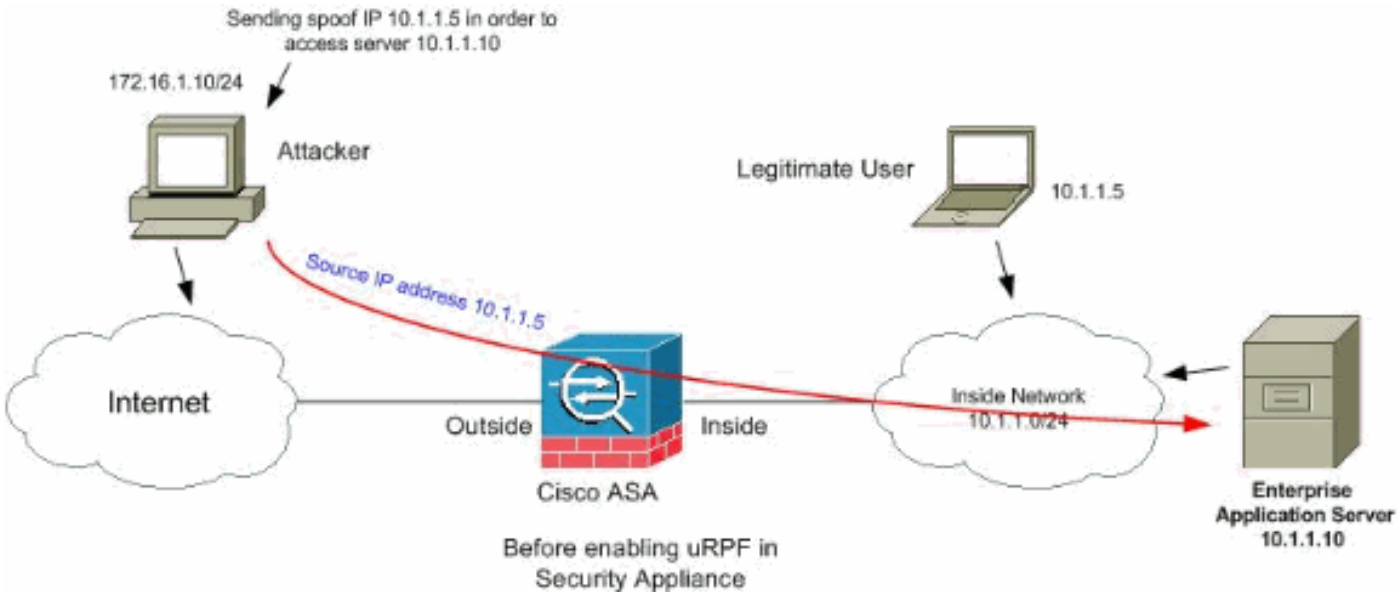
- ICMP-pakketten hebben geen sessie, dus wordt elk pakket gecontroleerd.
- UDP en TCP hebben sessies, dus het eerste pakket vereist een omgekeerde routeraadpleging. Andere pakketten die tijdens de sessie worden ontvangen, worden gecontroleerd met behulp van een bestaande status die als onderdeel van de sessie wordt onderhouden. Niet-aanvankelijke pakketten worden gecontroleerd om te verzekeren dat zij op de zelfde interface aankwamen die door het eerste pakket wordt gebruikt.

Typ deze opdracht om Unicast RPF in te schakelen:

```
hostname(config)#ip verify reverse-path interface interface_name
```

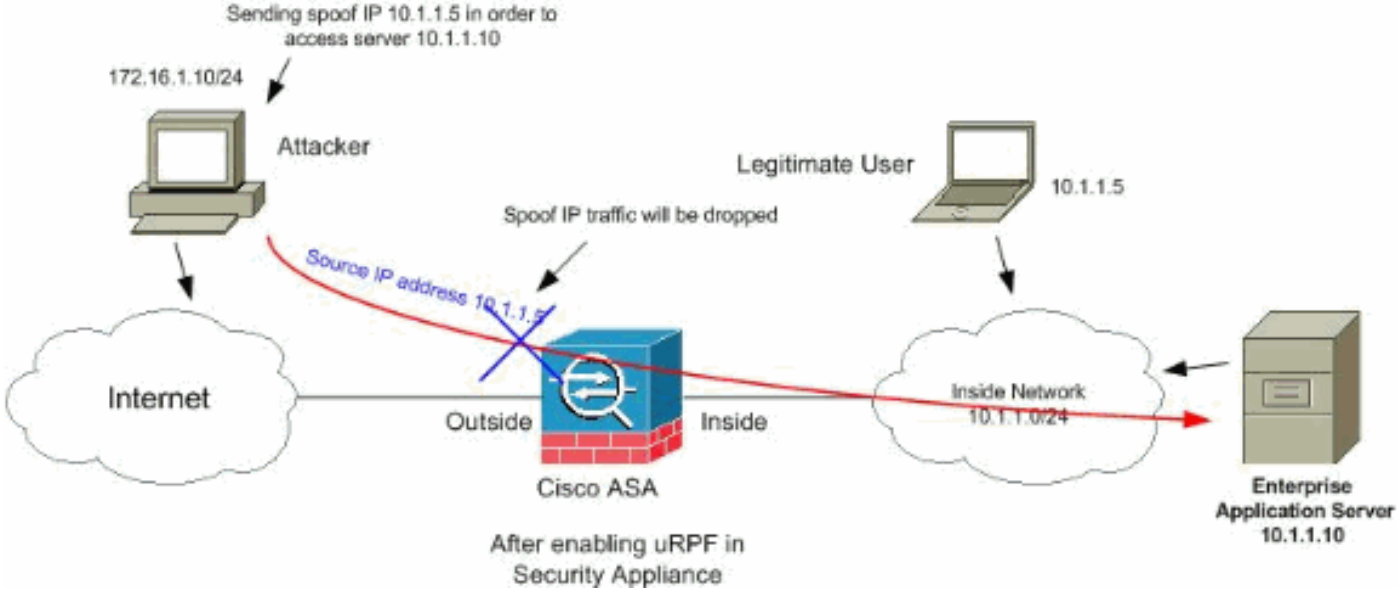
Voorbeeld:

Zoals dit cijfer wordt getoond, begint de PC van de aanvaller een verzoek aan de toepassingsserver 10.1.1.10 door een pakket met een vervalst bron IP adres 10.1.1.5/24 te verzenden, en de server verstuurt een pakket naar het echte IP adres 10.1.1.5/24 in antwoord op het verzoek. Dit type illegaal pakket zal zowel de toepassingsserver als de legitieme gebruiker in het binnennetwerk aanvallen.



Unicast RPF kan aanvallen op basis van bronadresspoofing verhinderen. U dient de uRPF in de externe interface van de ASA te configureren zoals hier wordt getoond:

```
ciscoasa(config)#ip verify reverse-path interface outside
```



Identificatie van spoelwater met behulp van systeemmeldingen

Het security apparaat blijft syslogfoutmeldingen ontvangen, zoals aangegeven in de afbeelding. Dit wijst op mogelijke aanvallen met gespoofed pakketten of die wegens asymmetrische routing zouden kunnen veroorzaken.

1.

```
%PIX|ASA-2-106001: Inbound TCP connection denied from IP_address/port
to IP_address/port flags tcp_flags on interface interface_name
```

verklaringDit is een verbinding-gerelateerd bericht. Dit bericht verschijnt wanneer een poging om verbinding te maken met een intern adres wordt ontkend door het beveiligingsbeleid dat is gedefinieerd voor het gespecificeerde type verkeer. Mogelijke waarden van *tcp_flags* komen overeen met de vlaggen in de TCP header die aanwezig waren toen de verbinding

werd ontkend. Bijvoorbeeld, een TCP pakket gearriveerd waarvoor geen verbindingsstaat in het veiligheidsapparaat bestaat, en het werd ingetrokken. De *tcp_flags* in dit pakje zijn FIN en ACK.De *tcp_flags* waren als volgt:ACK-het ontvangstnummer is ontvangen.FIN-Data werd verzonden.PSH — De ontvanger gaf gegevens door aan de applicatie.RST-De verbinding werd opnieuw ingesteld.SYN-Volgnummers werden gesynchroniseerd om een verbinding te starten.URG-De urgent pointer werd geldig verklaard.Er zijn veel redenen om de PIX/ASA niet te gebruiken voor statische vertalingen. Maar, een algemene reden is als de gedemilitariseerde zone (DMZ) interface is geconfigureerd met hetzelfde beveiligingsniveau (0) als de externe interface.Om deze kwestie op te lossen, moet u een ander veiligheidsniveau aan alle interfaces toewijzenRaadpleeg Interfaceparameters configureren voor meer informatie.Deze foutmelding wordt ook weergegeven als een extern apparaat een IDENT-pakket naar de interne client verstuurt, dat door de PIX-firewall is gevallen. Raadpleeg PIX-prestatieproblemen veroorzaakt door IDENT-protocol voor meer informatie

2.

```
%PIX|ASA-2-106007: Deny inbound UDP from outside_address/outside_port
to inside_address/inside_port due to DNS {Response|Query}
```

verklaringDit is een verbinding-gerelateerd bericht. Dit bericht wordt weergegeven als de gespecificeerde verbinding mislukt vanwege een **uitgaande ontkenningsopdracht**. De protocolvariabele kan ICMP, TCP of UDP zijn.**Aanbevolen actie:** Gebruik de opdracht **Uitvoer tonen** om uitgaande lijsten te controleren.

3.

```
%PIX|ASA-3-106014: Deny inbound icmp src interface_name: IP_address dst
interface_name: IP_address (type dec, code dec)
```

verklaringHet security apparaat ontkent elke inkomende ICMP-pakkettoegang. Standaard worden alle ICMP-pakketten geweigerd, tenzij dit specifiek is toegestaan.

4.

```
%PIX|ASA-2-106016: Deny IP spoof from (IP_address) to IP_address on
interface interface_name.
```

verklaringDit bericht wordt gegenereerd wanneer een pakket arriveert op de interface van het beveiligingsapparaat met een IP-adres van de bestemming van 0.0.0.0 en een MAC-adres van de interface van het security apparaat. Daarnaast wordt dit bericht gegenereerd wanneer het security apparaat een pakje met een ongeldig bronadres heeft weggegooid, dat een van de volgende of een ander ongeldig adres kan bevatten:Loopback-netwerk (127.0.0.0)Uitzenden (beperkt, op net gericht, op net gericht, en op alle subnetten gericht)De bestemmingslocatie (land.c)Om de pakketdetectie vanuit een punt verder te verbeteren, gebruikt u de opdracht **icmp** om het security apparaat te configureren om pakketten weg te gooien met bronadressen die bij het interne netwerk horen. Dit komt doordat de opdracht **toegangslijsten** is afgekeurd en niet langer gegarandeerd is om correct te werken.**Aanbevolen actie:** Bepaal of een externe gebruiker probeert het beveiligde netwerk aan te tasten. Controleer op verkeerde klanten.

5.

```
%PIX|ASA-2-106017: Deny IP due to Land Attack from IP_address to
IP_address
```

verklaringHet security apparaat heeft een pakket ontvangen met het IP-bronadres, gelijk aan de IP-bestemming en de doelpoort gelijk aan de bronpoort. Dit bericht geeft een spoofed pakje aan dat is ontworpen om systemen aan te vallen. Deze aanval wordt een landaanval genoemd.**Aanbevolen actie:** Als dit bericht blijft bestaan, wordt mogelijk een aanval uitgevoerd. Het pakket geeft niet genoeg informatie om te bepalen waar de aanval vandaan

komt.

6.
```
%PIX|ASA-1-106021: Deny protocol reverse path check from
source_address to dest_address on interface interface_name
```
verklaringEen aanval is in gang gezet. Iemand probeert een IP-adres op een inkomende verbinding te plaatsen. Unicast RPF, ook gekend als omgekeerde route raadpleging, ontdekte een pakket dat geen bronadres heeft dat door een route wordt vertegenwoordigd en veronderstelt dat het deel van een aanval op uw veiligheidsapparaat uitmaakt.Dit bericht verschijnt wanneer u Unicast RPF met de IP verify-opdracht hebt ingeschakeld. Deze functie werkt op pakketten die naar een interface worden ingevoerd. Als dit aan de buitenkant is ingesteld, controleert het beveiligingsapparaat welke pakketten van buitenaf zijn aangekomen.Het veiligheidsapparaat kijkt omhoog op een route gebaseerd op het bronadres. Als er geen entry gevonden wordt en er geen route gedefinieerd wordt, verschijnt dit logbericht van het systeem en de verbinding komt neer.Als er een route is, controleert het beveiligingsapparaat welke interface er is. Als het pakket op een andere interface is gearriveerd, is het of een punt of is er een asymmetrische routeringsomgeving die meer dan één pad naar een bestemming heeft. Het security apparaat ondersteunt geen asymmetrische routing.Als het security apparaat op een interne interface is geconfigureerd, controleert het de statische opdrachtverklaringen van de route of RIP. Als het bronadres niet gevonden is, spaart een interne gebruiker hun adres.Aanbevolen actie: Ook al is een aanval gaande, als deze optie is ingeschakeld, is er geen gebruikersactie vereist. Het veiligheidsapparaat neemt de aanval af.Opmerking: de opdracht asp tonen de pakketten of verbindingen die door het accelerated security pad (asp) zijn gevallen, wat u kan helpen om een probleem op te lossen. Het geeft ook aan wanneer de laatste keer dat de ASP-tellers werden geklaard. Gebruik de opdracht Show asp-stop-met voorverf-overtreden opdracht waarin de teller wordt verhoogd wanneer ip verify reverse-pad op een interface is geconfigureerd en het security apparaat een pakket ontvangt waarvoor de routeweergave van de bron-IP niet dezelfde interface oplevert als het pakket dat werd ontvangen.
```
ciscoasa#show asp drop frame rpf-violated
  Reverse-path verify failed                       2
```
Opmerking: Aanbeveling: Pak de bron van het verkeer vast op basis van de bron-IP die in dit volgende systeembericht is afgedrukt en onderzoek waarom het spoofed-verkeer verzenden.Opmerking: Systeemlogberichten: 106021

7.
```
%PIX|ASA-1-106022: Deny protocol connection spoof from source_address
to dest_address on interface interface_name
```
verklaringEen pakket dat een verbinding aansluit, komt op een andere interface dan de interface waar de verbinding begon.Als een gebruiker bijvoorbeeld een verbinding start op de interne interface, maar het security apparaat detecteert dezelfde verbinding die aankomt op een perimeter, dan heeft het security apparaat meer dan één pad naar een bestemming. Dit staat bekend als asymmetrische routing en wordt niet ondersteund op het security apparaat.Een aanvaller zou ook kunnen proberen pakketten van de ene aansluiting op de andere toe te voegen als manier om te breken in het beveiligingsapparaat. In beide gevallen geeft het beveiligingsapparaat dit bericht weer en valt de verbinding af.Aanbeveling: Dit bericht verschijnt wanneer de ip verify-opdracht niet is ingesteld. Controleer of de routing niet asymmetrisch is.

8.
```
%PIX|ASA-4-106023: Deny protocol src
[interface_name:source_address/source_port] dst
interface_name:dest_address/dest_port [type {string}, code {code}] by
```

```
access_group acl_ID
```

verklaringEen IP-pakket werd ontkend door ACL. Dit bericht toont zelfs als u de **logoptie** niet voor ACL hebt ingeschakeld.**Aanbeveling:** Als de berichten vanaf hetzelfde bronadres blijven staan, kunnen de berichten duiden op een poging om te voet of de poort te scannen. Neem contact op met de externe hostbeheerders.

9.
```
%PIX|ASA-3-210011: Connection limit exceeded cnt/limit for dir packet
from sip/sport to dip/dport on interface if_name.
```

10.
```
%ASA-4-419002: Received duplicate TCP SYN from
in_interface:src_address/src_port to out_interface:dest_address/dest_port with
different initial sequence number.
```

verklaringDit systeemlogbericht geeft aan dat het opzetten van een nieuwe verbinding door het firewallapparaat zal leiden tot het overschrijden van ten minste één van de ingestelde maximale verbindingsgrenzen. Het systeemlogbericht is zowel van toepassing op verbindingsgrenzen die zijn geconfigureerd met behulp van een statische opdracht, als op beperkingen die zijn ingesteld met behulp van Cisco modulair beleidskader. De nieuwe verbinding wordt door het firewallapparaat niet toegestaan totdat een van de bestaande verbindingen is afgebroken, waardoor de huidige connectie onder het ingestelde maximum komt te liggen.*cent*—Huidige connectie-telling*limiet*-ingesteld verbindingslimiet*dir*-richting van verkeer, inkomende of uitgaandeIP-adres bron*sport*—bronpoort*IP*-adres bestemming*poort*—bestemming*if_name*—Naam van de interface waarop de verkeerseenheid is ontvangen, Primair of Secundair.**Aanbeveling:** Omdat de verbindingsgrenzen om een goede reden worden geconfigureerd kon dit systeemlogbericht wijzen op een mogelijke DoS-aanval, in welk geval de bron van het verkeer waarschijnlijk een gespoofd IP-adres is. Als het IP-adres van de bron niet volledig willekeurig is, kan het selecteren van de bron en het blokkeren ervan met behulp van een toegangslijst helpen. In andere gevallen zou het krijgen van snuffelsporen en het analyseren van de bron van het verkeer helpen om ongewenste verkeer te isoleren van legaal verkeer.

Basisdetectie van bedreigingen in ASA 8.x

Cisco security applicatie ASA/PIX ondersteunt de functie die bedreigingsdetectie heet, van softwareversie 8.0 en hoger. Gebruik van basisdetectie, controleert het security apparaat het aantal verzonden pakketten en beveiligingsgebeurtenissen om deze redenen:

- Ontkennen door toegangslijsten
- Slechte pakketindeling (zoals ongeldige-ip-header of ongeldige-tcp-hdr-lengte)
- Verbindingsgrenzen overschreden (zowel voor het hele systeem gelden beperkingen als beperkingen die in de configuratie zijn ingesteld)
- DoS-aanval gedetecteerd (zoals een ongeldige SPI, stateful Firewall check defect)
- Basis controles van de firewall hebben gefaald (Deze optie is een gecombineerd tarief dat alle aan firewall gerelateerde pakketdalingen in deze lijst omvat. Dit bevat geen items die gerelateerd zijn aan firewalls, zoals interfaceoverload, pakketten die niet zijn verontreinigd bij de toepassingsinspectie en scanaanval.)
- Verdachte ICMP-pakketten gedetecteerd
- Packet is niet bij toepassing geïnspecteerd
- Interface-overbelasting
- Scaningaanval gedetecteerd (Deze optie controleert scanaanvallen; Het eerste TCP-pakket is

bijvoorbeeld geen SYN-pakket, of de TCP-verbinding heeft de 3-voudige handdruk gefaald. De volledige detectie van de scandreiging (raadpleeg de scandetectie van bedreigingen voor meer informatie te configureren) neemt deze informatie over de scanaanval in en treedt hierop in door hosts als aanvallers te classificeren en deze automatisch te verzenden, bijvoorbeeld).
- Onvolledige sessiedetectie zoals TCP SYN-aanval gedetecteerd of geen UDP-sessieaanval gedetecteerd.

Wanneer het veiligheidsapparaat een bedreiging detecteert, verstuurt het onmiddellijk een systeemlogbericht (730100).

De basisdetectie van bedreigingen beïnvloedt de prestaties alleen wanneer er druppels of potentiële bedreigingen zijn. Zelfs in dit scenario is de impact op de prestaties onbeduidend.

De opdracht **Show Threat-Detectiesnelheid** wordt gebruikt om mogelijke aanvallen te identificeren wanneer u in het security apparaat bent aangemeld.

```
ciscoasa#show threat-detection rate
                         Average(eps)    Current(eps) Trigger      Total events
  10-min ACL  drop:                 0               0       0                16
  1-hour ACL  drop:                 0               0       0               112
  1-hour SYN attck:                 5               0       2             21438
  10-min  Scanning:                 0               0      29               193
  1-hour  Scanning:               106               0      10            384776
  1-hour Bad  pkts:                76               0       2            274690
  10-min  Firewall:                 0               0       3                22
  1-hour  Firewall:                76               0       2            274844
  10-min DoS attck:                 0               0       0                 6
  1-hour DoS attck:                 0               0       0                42
  10-min Interface:                 0               0       0               204
  1-hour Interface:                88               0       0            318225
```

Raadpleeg het gedeelte Basisdetectie van bedreigingen van de ASA 8.0-configuratiehandleiding voor meer informatie over het configuratie-onderdeel.

Syrische boodschap 733100

Fout:

```
%ASA-4-733100: Object drop rate rate_ID exceeded. Current burst rate is rate_val per second, max
configured rate is rate_val; Current average rate is rate_val per second, max configured rate is
rate_val; Cumulative total count is total_cnt
```

Het gespecificeerde object in het systeemlogbericht heeft de gespecificeerde barstdrempelsnelheid of gemiddelde drempelsnelheid overschreden. Het object kan een lagere activiteit van een host-, TCP/UDP-poort, IP-protocol of verschillende druppels zijn vanwege mogelijke aanvallen. Het geeft aan dat het systeem mogelijk wordt aangevallen.

Opmerking: Deze foutmeldingen met resolutie zijn alleen van toepassing op ASA 8.0 en hoger.

1. Object-De algemene of speciale bron van een daling rate teller, die deze kan bevatten:FirewallSlechte pkksSnelheidslimietDoS-aanvalACL-trapConn-limietICMP-toetsScannenSYN-aanvalinspecterenInterface
2. rate_ID—de geconfigureerde snelheid die wordt overschreden. De meeste objecten kunnen met maximaal drie verschillende snelheden worden ingesteld voor verschillende intervallen.
3. rate_val—een bepaalde waarde.

4. total_cnt—De totale telling sinds het object is aangemaakt of gewist.

Deze drie voorbeelden laten zien hoe deze variabelen zich voordoen:

- Voor een interface-uitval vanwege een CPU- of busbeperking:

```
%ASA-4-733100: [Interface] drop rate 1 exceeded. Current burst rate is 1 per
    second,
max configured rate is 8000; Current average rate is 2030 per second,
max configured rate is 2000; Cumulative total count is 3930654
```

- Voor een scandaling als gevolg van mogelijke aanvallen:

```
ASA-4-733100: [Scanning] drop rate-1 exceeded. Current burst rate is 10 per
    second_
max configured rate is 10; Current average rate is 245 per second_
max configured rate is 5; Cumulative total count is 147409 (35 instances received)
```

- Voor slechte pakketten door mogelijke aanvallen:

```
%ASA-4-733100: [Bad pkts] drop rate 1 exceeded. Current burst rate is 0 per
    second,
max configured rate is 400; Current average rate is 760 per second,
max configured rate is 100; Cumulative total count is 1938933
```

Aanbevolen actie:

Voer deze stappen uit volgens het opgegeven objecttype dat in het bericht verschijnt:

1. Als het object in het syslog-bericht een van de volgende waarden heeft:FirewallSlechte pkksSnelheidslimietDodeS-aanvalACL-trapConn-limietICMP-toetsScannenSYN-aanvalinspecterenInterfaceControleer of de uitvalsnelheid voldoende is voor de wasomgeving.
2. Stel het drempelpercentage van de specifieke uitval in op een geschikte waarde door de opdracht **voor** de **detectie van bedreigingen** uit te voeren**, waarbij** *xxx* een van deze *opties* is:druppelonverpaktebeperkingdruppelvalijskappendruppelinterfacemodulesscandreigingsyn-aanval
3. Als het object in het syslogbericht een TCP- of UDP-poort, een IP-protocol of een host-uitloop is, controleert u of de uitrolsnelheid aanvaardbaar is voor de actieve omgeving.
4. Pas de drempelsnelheid van de bepaalde daling in een aangewezen waarde aan door de **dreigen-detectie** opdracht **toe te passen**. Raadpleeg het gedeelte Basisdetectie van bedreigingen van de ASA 8.0 Configuration voor meer informatie.

Opmerking: Als u niet wilt dat de uitrolsnelheid hoger is dan de waarschuwing, kunt u deze uitschakelen door de opdracht **Geen** bedreigingen**-detectie basisbedreigingen** uit te voeren.

Gerelateerde informatie

- Cisco 5500 Series ondersteuningspagina voor adaptieve security applicaties
- Cisco 500 Series PIX-ondersteuningspagina
- Verdediging tegen TCP-overstroming
- Cisco Applied Mitiging Bulletin: Identificatie en beperking van de exploitatie van de Denial of Service-kwetsbaarheden in de module voor contentswitching
- Cisco Applied Mitiging Bulletin: Het identificeren en beperken van exploitatie van de meervoudige kwaliteiten in Cisco PIX en ASA applicaties en firewall-servicesmodule
- IP-pakketten
- Technische ondersteuning en documentatie – Cisco Systems