Het Zone-Based Policy Firewall Design begrijpen

Inhoud

Inleiding

Dit document beschrijft het configuratiemodel voor de functieset Cisco IOS® Firewall, Zone-based Policy Firewall (ZFW).

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

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 zorgen dat u de potentiële impact van elke opdracht begrijpt.

Conventies

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

Achtergrondinformatie

Dit nieuwe configuratiemodel biedt intuïtief beleid voor meerdere interfacerouters, verhoogde granulariteit van de toepassing van het firewallbeleid, en een standaard deny-all beleid dat verkeer tussen firewall-beveiligingszones verbiedt totdat een expliciet beleid wordt toegepast om gewenst verkeer toe te staan.

Bijna alle klassieke Cisco IOS-firewallfuncties die zijn geïmplementeerd voordat Cisco IOS-softwarerelease 12.4(6)T worden ondersteund in de nieuwe op zones gebaseerde beleidsinspectieinterface:

- Stateful pakketinspectie
- VRF-bewuste Cisco IOS-firewall
- URL-filtering
- Beperking van weigeringen van services (DoS)

Cisco IOS-softwarerelease 12.4(9)T heeft ZFW-ondersteuning toegevoegd voor sessies/verbindingen en doorvoerbeperkingen per klasse, evenals toepassingsinspectie en controle:

- HTTP
- Post Office Protocol (POP3), Internet Mail Access Protocol (IMAP), Simple Mail Transfer Protocol/Enhanced Simple Mail Transfer Protocol (SMTP/ESMTP)
- Sun Remote Procedure Call (RPC)
- IM-toepassingen (Instant Messaging):Microsoft MessengerYahoo! MessengerAOL Instant Messenger
- Peer-to-peer (P2P) bestanden delen:bittorrentKaZaGnutellaeDonkey

Cisco IOS-softwarerelease 12.4(11)T heeft statistieken toegevoegd voor een eenvoudiger afstemming van DoS-bescherming.

Sommige functies en mogelijkheden van Cisco IOS Classic Firewall worden nog niet ondersteund in een ZFW in Cisco IOS-softwarerelease 12.4(15)T:

- Verificatieproxy
- Stateful firewall-failover
- Unified firewall MIB
- IPv6-stateful inspectie
- Ondersteuning van TCP buiten bedrijf

ZFW verbetert over het algemeen Cisco IOS-prestaties voor de meeste activiteiten met betrekking tot firewallinspectie. Noch Cisco IOS ZFW noch Classic Firewall biedt stateful inspection ondersteuning voor multicast verkeer.

Zone-Based Policy - Overzicht

Stateful inspection voor Cisco IOS Classic Firewall (voorheen bekend als Context-Based Access Control of CBAC) maakte gebruik van een op interfaces gebaseerd configuratiemodel, waarin een stateful inspection beleid is toegepast op een interface. Alle verkeerspassen door die interface kregen hetzelfde inspectiebeleid. Dit configuratiemodel beperkte de granulariteit van het firewallbeleid en veroorzaakte verwarring van de juiste toepassing van firewallbeleid, in het bijzonder in scenario's wanneer het firewallbeleid tussen meerdere interfaces moet worden toegepast.

Zone-Based Policy Firewall (ook bekend als Zone-Policy Firewall, of ZFW) wijzigt de firewallconfiguratie van het oudere op interfaces gebaseerde model in een flexibeler, gemakkelijker te begrijpen op zones gebaseerd model. De interfaces worden toegewezen aan zones, en het inspectiebeleid wordt toegepast op verkeer dat zich tussen de zones beweegt. Het beleid tussen zones biedt aanzienlijke flexibiliteit en granulariteit, zodat er verschillende inspectiemaatregelen kunnen worden toegepast op meerdere hostgroepen die op dezelfde

routerinterface zijn aangesloten.

Het firewallbeleid wordt geconfigureerd met Cisco Policy Language (CPL), die een hiërarchische structuur gebruikt om inspectie te definiëren voor netwerkprotocollen en de groepen hosts waarop de inspectie kan worden toegepast.

Zone-Based Policy Configuration-model

ZFW wijzigt de manier waarop u een Cisco IOS-firewall-inspectie configureert volledig in vergelijking met de Cisco IOS Classic Firewall.

De eerste belangrijke verandering in de firewallconfiguratie is de introductie van op zone gebaseerde configuratie. Cisco IOS Firewall is de eerste eigenschap van de de bedreigingsdefensie van de Software van Cisco IOS om een model van de streekconfiguratie uit te voeren. Andere kenmerken kunnen het zonemodel in de loop der tijd overnemen. Het op Cisco IOS Classic Firewall-gebaseerde configuratiemodel met stateful inspection (of CBAC) dat gebruikmaakt van de opdrachtset voor IP-inspectie, wordt gedurende een bepaalde periode behouden. Er zijn echter maar weinig nieuwe functies die configureerbaar zijn met de klassieke opdrachtregelinterface (CLI). ZFW gebruikt geen stateful inspection of CBAC commando's. De twee configuratiemodellen kunnen gelijktijdig op routers worden gebruikt, maar niet op interfaces worden gecombineerd. Een interface kan niet worden geconfigureerd als een security zone lid en tegelijkertijd worden geconfigureerd voor IP-inspectie .

Zones stellen de beveiligingsgrenzen van uw netwerk in. Een zone definieert een grens waar verkeer aan beleidsbeperkingen wordt onderworpen wanneer het naar een ander gebied van uw netwerk gaat. Het standaardbeleid van ZFW tussen zones is ontkennen allen. Als geen beleid uitdrukkelijk wordt gevormd, wordt al verkeer dat zich tussen streken beweegt geblokkeerd. Dit is een belangrijke afwijking van stateful inspection model waarbij verkeer impliciet werd toegestaan tot expliciet geblokkeerd met een toegangscontrolelijst (ACL).

De tweede grote verandering is de introductie van een nieuwe taal voor configuratiebeleid die bekend staat als CPL. Gebruikers die bekend zijn met de Cisco IOS-softwarerelease Modular Quality-of-Service (QoS) CLI (MQC) kunnen herkennen dat het formaat vergelijkbaar is met het gebruik van QoS-klassekaarten om aan te geven welk verkeer wordt beïnvloed door de actie die in een beleidskaart wordt toegepast.

Regels voor zone-gebaseerde Policy Firewall-toepassing

Het lidmaatschap van de netwerkinterface van de router in streken is onderworpen aan verscheidene regels die interfacegedrag regeren, zoals het verkeer is dat zich tussen de interfaces van het streeklid beweegt:

- Een zone moet worden geconfigureerd voordat interfaces aan de zone kunnen worden toegewezen.
- Een interface kan aan slechts één veiligheidszone worden toegewezen.
- Al verkeer aan en van een bepaalde interface wordt impliciet geblokkeerd wanneer de interface aan een streek, behalve verkeer aan en van andere interfaces in de zelfde streek, en verkeer aan om het even welke interface op de router wordt toegewezen.
- Het verkeer is impliciet toegestaan om standaard te stromen tussen interfaces die lid zijn van dezelfde zone.

- Om verkeer van en naar een interface van een zonelid toe te laten, moet een beleid dat verkeer toestaat of inspecteert tussen die zone en een andere zone worden geconfigureerd.
- De zelfzone is de enige uitzondering op de standaard ontkennen alle beleid. Al verkeer aan om het even welke routerinterface wordt toegestaan tot het verkeer uitdrukkelijk wordt ontkend.
- Het verkeer kan niet tussen een interface van het streeklid en om het even welke interface stromen die geen streeklid is. Pas, inspecteer, en laat vallen acties kan slechts tussen twee zones worden toegepast.
- Interfaces die niet aan een zone zijn toegewezen, fungeren als klassieke routerpoorten en kunnen nog steeds klassieke stateful inspection/CBAC-configuratie gebruiken.
- Als het vereist is dat een interface op de box geen deel uitmaakt van het zone/firewall beleid. Het kan nog steeds noodzakelijk zijn om die interface in een zone te plaatsen en een pas te vormen al beleid (een soort dummy beleid) tussen die zone en een andere zone waaraan verkeersstroom wordt gewenst.
- Uit het vorige gedrag volgt dat als er verkeer tussen alle interfaces in een router moet stromen, alle interfaces deel moeten uitmaken van het zoningmodel (elke interface moet lid zijn van een of andere zone).
- De enige uitzondering op het vorige gedrag, ontken door gebrek benadering is het verkeer aan en van de router, die door gebrek wordt toegelaten. Een expliciet beleid kan worden geconfigureerd om dergelijk verkeer te beperken.

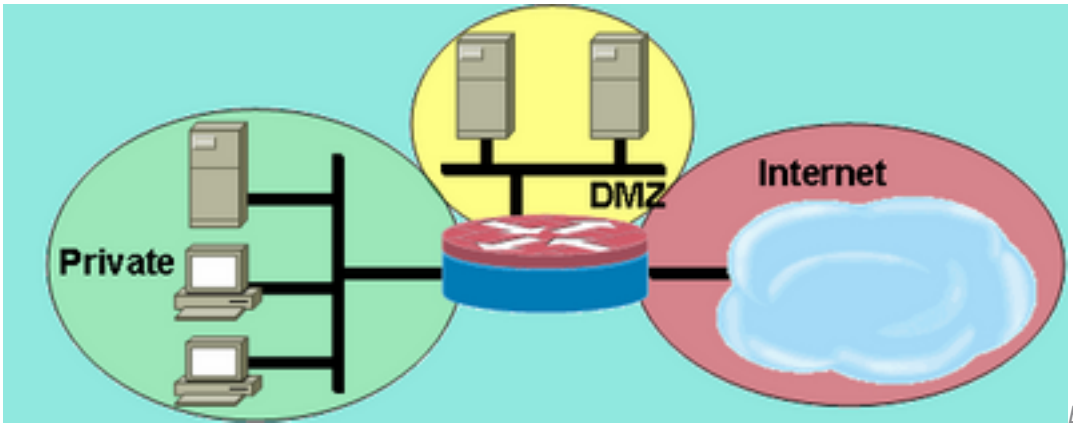
Design Zone-gebaseerde beleidsnetwerkbeveiliging

Een veiligheidszone moet voor elk gebied van relatieve veiligheid binnen het netwerk worden geconfigureerd, zodat alle interfaces die aan dezelfde zone zijn toegewezen, met een vergelijkbaar beveiligingsniveau worden beschermd. Neem bijvoorbeeld een toegangsrouter met drie interfaces:

- Eén interface met het openbare internet
- Eén interface die is aangesloten op een privaat LAN dat niet via het openbare internet toegankelijk mag zijn
- Eén interface die is verbonden met een gedemilitariseerde zone voor internetdiensten (DMZ), waar een webserver, DNS-server (Domain Name System) en e-mailserver toegankelijk moeten zijn voor het openbare internet

Elke interface in dit netwerk wordt toegewezen aan zijn eigen zone, hoewel u gevarieerde toegang van het openbare internet naar specifieke hosts in de DMZ en gevarieerd toepassingsgebruiksbeleid voor hosts in het beveiligde LAN kunt toestaan (zie afbeelding 1.)

Afbeelding 1: Basis Security Zone-topologie



Basis Security Zone-topologie

In dit voorbeeld heeft elke zone slechts één interface. Als een extra interface wordt toegevoegd aan de privé-zone, kunnen de hosts die zijn aangesloten op de nieuwe interface in de zone verkeer doorgeven aan alle hosts op de huidige interface in dezelfde zone. Bovendien wordt het hostverkeer naar hosts in andere zones op dezelfde manier beïnvloed door het huidige beleid.

Typisch, heeft het voorbeeldnetwerk drie belangrijke beleid:

- Privézone-verbinding met internet
- Private zone connectiviteit naar DMZ-hosts
- Internetzone-connectiviteit met DMZ-hosts

Omdat DMZ wordt blootgesteld aan het openbare internet, kunnen de DMZ-hosts worden blootgesteld aan ongewenste activiteit van kwaadwillige individuen die er in kunnen slagen om één of meerdere DMZ-hosts te beschadigen. Als er geen toegangsbeleid is voorzien voor DMZ-hosts om zowel privézone-hosts als internetzone-hosts te bereiken, dan kunnen de personen die de DMZ-hosts hebben gecompromitteerd de DMZ-hosts niet gebruiken om verdere aanvallen uit te voeren tegen private of internet-hosts. ZFW legt een prohibitieve standaardveiligheidshouding op. Daarom, tenzij de gastheren DMZ specifiek worden verleend toegang tot andere netwerken, worden andere netwerken beschermd tegen om het even welke verbindingen van de gastheren DMZ. Op dezelfde manier wordt geen toegang voor de gastheren van Internet verstrekt om tot de privé zonegastheren toegang te hebben, zodat zijn de privé zonegastheren veilig van ongewenste toegang door de gastheren van Internet.

Gebruik IPSec VPN met zone-gebaseerde beleidsfirewall

Recente verbeteringen van IPSec VPN vereenvoudigen de configuratie van firewallbeleid voor VPN-connectiviteit. Met IPSec Virtual Tunnel Interface (VTI) en GRE+IPSec kunt u VPN site-to-site- en clientverbindingen beperken tot een specifieke beveiligingszone door de tunnelinterfaces in een gespecificeerde beveiligingszone te plaatsen. De verbindingen kunnen in VPN DMZ worden geïsoleerd als de connectiviteit door een specifiek beleid moet worden beperkt. Of, als de connectiviteit van VPN impliciet wordt vertrouwd op, kan de connectiviteit van VPN in de zelfde veiligheidszone worden geplaatst zoals het vertrouwde binnen netwerk.

Als een niet-VTI IPSec wordt toegepast, vereist het beleid van de de connectiviteitsfirewall van VPN nauwkeurig toezicht om veiligheid te handhaven. Het gebiedsbeleid moet specifiek toegang door een IP adres voor verre plaatsgastheren of de cliënten van VPN toestaan als de veilige gastheren in een verschillende streek dan de VPN cliënt gecodeerde verbinding aan de router zijn. Als het toegangsbeleid niet goed is geconfigureerd, kunnen hosts die moeten worden beschermd worden blootgesteld aan ongewenste, potentieel vijandige hosts. Raadpleeg VPN gebruiken met Zone-Based Policy Firewall voor verdere concept- en configuratiediscussies.

Configuratie van Cisco Policy Language (CPL)

Deze procedure kan worden gebruikt om een ZFW te configureren. De opeenvolging van stappen is niet belangrijk, maar sommige gebeurtenissen moeten in orde worden voltooid. Bijvoorbeeld, moet u een klasse-kaart vormen alvorens u een klasse-kaart aan een beleid-kaart toewijst. Op dezelfde manier kunt u geen beleid-kaart aan een streek-paar toewijzen tot u het beleid hebt gevormd. Als u probeert om een sectie te vormen die zich op een ander gedeelte van de configuratie baseert dat u niet hebt gevormd, antwoordt de router met een foutenmelding.

1. Definieer zones.
2. Bepaal zone-paren.
3. Definieer klasse-kaarten die verkeer beschrijven dat beleid moet hebben toegepast aangezien het een zone-paar kruist.
4. Definieer beleidskaarten om actie toe te passen op uw class-maps verkeer.
5. Pas beleidskaarten toe op zoneparen.
6. Wijs interfaces toe aan zones.

Op zone gebaseerde beleidsfirewall-klasse-kaarten configureren

Class-maps definiëren het verkeer dat door de firewall wordt geselecteerd voor beleidsapplicatie. Layer 4 class-maps sorteren het verkeer op basis van deze hier genoemde criteria. Deze criteria worden gespecificeerd met het matchbevel in een klasse-kaart:

- Toegangsgroep — Met een standaard, uitgebreide of benoemde ACL kan verkeer worden gefilterd op basis van IP-adres van de bron en de bestemming en de bron- en doelpoort.
- Protocol — Layer 4-protocollen (TCP, UDP en ICMP) en toepassingsservices zoals HTTP, SMTP, DNS en dergelijke, kunnen worden gespecificeerd voor elke bekende of door de gebruiker gedefinieerde service die bekend is bij poorttoewijzingen.
- Class-map — Een ondergeschikte class-map die extra matchcriteria biedt, kan worden genest binnen een andere class-map.
- Niet — Het criterium Not specificeert dat verkeer dat niet overeenkomt met een gespecificeerde service (protocol), toegangsgroep of ondergeschikte class-map is geselecteerd voor de class-map.

Criteria 'matching' combineren: "Match-Any" versus "Match-All"

Klasse-maps kunnen match-any of match-all operatoren toepassen om te bepalen hoe de match criteria moeten worden toegepast. Als match-any is opgegeven moet traffic aan slechts één van de matchcriteria in de class-map voldoen. Als match-all is opgegeven moet traffic voldoen aan alle class-map criteria om tot die bepaalde class te behoren.

De criteria van de overeenkomst moeten worden toegepast in volgorde van specifieker naar minder specifiek als het verkeer aan meerdere criteria voldoet. Neem bijvoorbeeld deze class-map:

```
class-map type inspect match-any my-test-cmap
 match protocol http
 match protocol tcp
```

HTTP-verkeer moet het matchprotocol http eerst ontmoeten om er zeker van te zijn dat het

verkeer wordt verwerkt door de servicespecifieke functies van HTTP-inspectie. Als de matchlijnen worden omgekeerd, zodat het verkeer de verklaring van TCP van het matchprotocol ontmoet alvorens het om protocol http te vergelijken, wordt het verkeer eenvoudig geclassificeerd als verkeer van TCP, en geïnspecteerd gebaseerd op de mogelijkheden van de component van de Inspectie van TCP van de Firewall. Dit is een probleem voor bepaalde services zoals FTP, TFTP en verschillende multimedia- en spraaksignaleringsservices zoals H.323, SIP, Skinny, RTSP en anderen. Deze diensten vereisen extra inspectiecapaciteit om de complexere activiteiten van deze diensten te kunnen herkennen.

ACL toepassen als overeenkomende criteria

Klasse-maps kunnen een ACL toepassen als een van de matchcriteria voor beleidstoepassing. Als een class-map alleen met criterium overeenkomt een ACL is en de class-map is gekoppeld aan een policy-map die de inspectie-actie toepast, past de router TCP- of UDP-basisinspectie toe voor al het verkeer dat door de ACL is toegestaan, behalve dat welke ZFW toepassingsbewuste inspectie biedt. Dit omvat (maar is niet beperkt tot) FTP, SIP, Skinny (SCCP), H.323, Sun RPC en TFTP. Als toepassingsspecifieke inspectie beschikbaar is en de ACL het primaire of controlekanaal toestaat, wordt om het even welk secundair of mediakanaal verbonden aan de primaire/controle toegestaan, ongeacht of de ACL het verkeer toestaat.

Als een class-map alleen ACL 101 toepast als de matchcriteria, wordt een ACL 101 als volgt weergegeven:

```
access-list 101 permit ip any any
```

Al verkeer wordt toegestaan in de richting van het dienst-beleid dat op een bepaald streek-paar wordt toegepast, en het terugkeerverkeer dat aan dit beantwoordt wordt toegestaan in de tegenovergestelde richting. Daarom moet ACL de beperking toepassen om verkeer tot specifieke gewenste types te beperken. Bericht dat de PAM- lijst toepassingsdiensten zoals HTTP, NetBIOS, H.323, en DNS omvat. Ondanks de kennis van PAM van het specifieke toepassingsgebruik van een bepaalde haven, past de firewall slechts voldoende toepassingsspecifieke capaciteit toe om aan de bekende eisen van het toepassingsverkeer te voldoen. Aldus, worden het eenvoudige toepassingsverkeer zoals telnet, SSH, en andere enig-kanaals toepassingen geïnspecteerd als TCP, en hun statistieken worden gecombineerd in de output van het showbevel. Als applicatie-specifieke zichtbaarheid in netwerkactiviteit gewenst is, moet u inspectie voor services configureren op naam van de applicatie (configureer match protocol HTTP, match protocol telnet, enzovoort).

Vergelijk de statistieken die beschikbaar zijn in de show policy-map type inspecteren zone-paar opdrachtoutput van deze configuratie met het meer expliciete firewallbeleid dat verderop op op de pagina wordt getoond. Deze configuratie wordt gebruikt om verkeer vanaf een Cisco IP-telefoon te controleren en om verschillende werkstations te selecteren die gebruik maken van een scala aan verkeer, waaronder HTTP, FTP, NetBIOS, SSH en DNS:

```
class-map type inspect match-all all-private
 match access-group 101
!
policy-map type inspect priv-pub-pmap
 class type inspect all-private
  inspect
 class class-default
!
zone security private
```

```
zone security public
zone-pair security priv-pub source private destination public
 service-policy type inspect priv-pub-pmap
!
interface FastEthernet4
 ip address 172.16.108.44 255.255.255.0
 zone-member security public
!
interface Vlan1
 ip address 192.168.108.1 255.255.255.0
 zone-member security private
!
access-list 101 permit ip 192.168.108.0 0.0.0.255 any
```

Hoewel deze configuratie eenvoudig te definiëren is en geschikt is voor al het verkeer dat afkomstig is uit de privézone (zolang het verkeer de standaard, door PAM herkende bestemmingshavens in acht neemt), biedt het beperkte zichtbaarheid in de serviceactiviteit en biedt het geen mogelijkheid om de bandbreedte- en sessielimieten van ZFW toe te passen voor specifieke soorten verkeer. Deze show beleid-map type inspect zone-paar priv-pub opdrachtoutput is het resultaat van de vorige eenvoudige configuratie die alleen een vergunning IP [sub] elke ACL tussen zone-paren gebruikt. Zoals u kunt zien, wordt het meeste werkstationverkeer geteld in de basis-TCP- of UDP-statistieken:

```
stg-871-L#show policy-map type insp zone-pair priv-pub
Zone-pair: priv-pub

  Service-policy inspect : priv-pub-pmap

    Class-map: all-private (match-all)
      Match: access-group 101
      Inspect
        Packet inspection statistics [process switch:fast switch]
        tcp packets: [413:51589]
        udp packets: [74:28]
        icmp packets: [0:8]
        ftp packets: [23:0]
        tftp packets: [3:0]
        tftp-data packets: [6:28]
        skinny packets: [238:0]

        Session creations since subsystem startup or last reset 39
        Current session counts (estab/half-open/terminating) [3:0:0]
        Maxever session counts (estab/half-open/terminating) [3:4:1]
        Last session created 00:00:20
        Last statistic reset never
        Last session creation rate 2
        Maxever session creation rate 7
        Last half-open session total 0

    Class-map: class-default (match-any)
      Match: any
      Drop (default action)
        0 packets, 0 bytes
```

In tegenstelling, een gelijkaardige configuratie die toepassing-specifieke klassen toevoegt verstrekt meer korrelige toepassingsstatistieken en controle, en past nog de zelfde breedte van de diensten aan die in het eerste voorbeeld werd getoond wanneer u de laatste-kans klasse-kaart bepaalt die slechts ACL als laatste kans in beleid-kaart aanpast:

```
class-map type inspect match-all all-private
```

```
 match access-group 101
class-map type inspect match-all private-ftp
 match protocol ftp
 match access-group 101
class-map type inspect match-any netbios
 match protocol msrpc
 match protocol netbios-dgm
 match protocol netbios-ns
 match protocol netbios-ssn
class-map type inspect match-all private-netbios
 match class-map netbios
 match access-group 101
class-map type inspect match-all private-ssh
 match protocol ssh
 match access-group 101
class-map type inspect match-all private-http
 match protocol http
 match access-group 101
!
policy-map type inspect priv-pub-pmap
 class type inspect private-http
  inspect
 class type inspect private-ftp
  inspect
 class type inspect private-ssh
  inspect
 class type inspect private-netbios
  inspect
 class type inspect all-private
  inspect
 class class-default!
zone security private
zone security public
zone-pair security priv-pub source private destination public
 service-policy type inspect priv-pub-pmap
!
interface FastEthernet4
 ip address 172.16.108.44 255.255.255.0
 zone-member security public
!
interface Vlan1
 ip address 192.168.108.1 255.255.255.0
 zone-member security private
!
access-list 101 permit ip 192.168.108.0 0.0.0.255 any
```

De meer specifieke configuratie verstrekt deze wezenlijke korrelige output voor het show beleid-kaart type inspecteren zone-paar priv-pub bevel:

```
stg-871-L#sh policy-map type insp zone-pair priv-pub
 Zone-pair: priv-pub

   Service-policy inspect : priv-pub-pmap

     Class-map: private-http (match-all)
       Match: protocol http
       Match: access-group 101
       Inspect
         Packet inspection statistics [process switch:fast switch]
         tcp packets: [0:2193]

         Session creations since subsystem startup or last reset 731
         Current session counts (estab/half-open/terminating) [0:0:0]
```

```
    Maxever session counts (estab/half-open/terminating) [0:3:0]
    Last session created 00:29:25
    Last statistic reset never
    Last session creation rate 0
    Maxever session creation rate 4
    Last half-open session total 0

Class-map: private-ftp (match-all)
  Match: protocol ftp
  Inspect
    Packet inspection statistics [process switch:fast switch]
    tcp packets: [86:167400]
    ftp packets: [43:0]

    Session creations since subsystem startup or last reset 7
    Current session counts (estab/half-open/terminating) [0:0:0]
    Maxever session counts (estab/half-open/terminating) [2:1:1]
    Last session created 00:42:49
    Last statistic reset never
    Last session creation rate 0
    Maxever session creation rate 4
    Last half-open session total 0

Class-map: private-ssh (match-all)
  Match: protocol ssh
  Inspect
    Packet inspection statistics [process switch:fast switch]
    tcp packets: [0:62]

    Session creations since subsystem startup or last reset 4
    Current session counts (estab/half-open/terminating) [0:0:0]
    Maxever session counts (estab/half-open/terminating) [1:1:1]
    Last session created 00:34:18
    Last statistic reset never
    Last session creation rate 0
    Maxever session creation rate 2
    Last half-open session total 0

Class-map: private-netbios (match-all)
  Match: access-group 101
  Match: class-map match-any netbios
    Match: protocol msrpc
      0 packets, 0 bytes
      30 second rate 0 bps
    Match: protocol netbios-dgm
      0 packets, 0 bytes
      30 second rate 0 bps
    Match: protocol netbios-ns
      0 packets, 0 bytes
      30 second rate 0 bps
    Match: protocol netbios-ssn
      2 packets, 56 bytes
      30 second rate 0 bps
  Inspect
    Packet inspection statistics [process switch:fast switch]
    tcp packets: [0:236]

    Session creations since subsystem startup or last reset 2
    Current session counts (estab/half-open/terminating) [0:0:0]
    Maxever session counts (estab/half-open/terminating) [1:1:1]
    Last session created 00:31:32
    Last statistic reset never
    Last session creation rate 0
    Maxever session creation rate 1
```

```
    Last half-open session total 0

Class-map: all-private (match-all)
  Match: access-group 101
  Inspect
    Packet inspection statistics [process switch:fast switch]
    tcp packets: [51725:158156]
    udp packets: [8800:70]
    tftp packets: [8:0]
    tftp-data packets: [15:70]
    skinny packets: [33791:0]

    Session creations since subsystem startup or last reset 2759
    Current session counts (estab/half-open/terminating) [2:0:0]
    Maxever session counts (estab/half-open/terminating) [2:6:1]
    Last session created 00:22:21
    Last statistic reset never
    Last session creation rate 0
    Maxever session creation rate 12
    Last half-open session total 0

Class-map: class-default (match-any)
  Match: any
  Drop (default action)
    4 packets, 112 bytes
```

Een ander bijkomend voordeel voor het gebruik van een meer gedetailleerde klasse-kaart en policy-map configuratie, zoals eerder vermeld, is een mogelijkheid om klassespecifieke limieten toe te passen op sessie- en snelheidswaarden; en specifiek om inspectieparameters aan te passen door toepassing van een parameterkaart om elk klasse-inspectiegedrag aan te passen.

Op zone gebaseerde beleidsfirewallbeleidskaarten configureren

De policy-map past firewallbeleidsacties op een of meer class-maps toe om het service-beleid te definiëren dat wordt toegepast op een security zone-paar. Wanneer een inspect-type policy-map wordt gemaakt, wordt een standaardklasse met de naam class-default toegepast aan het einde van de klasse. De class-default beleidsactie is drop maar kan veranderd worden om over te gaan. De logoptie kan met de dalingsactie worden toegevoegd. Inspecteren kan niet toegepast worden bij class-default.

Zone-Based Policy Firewall-acties

ZFW voorziet in drie acties voor verkeer dat van de ene zone naar de andere verloopt:

- Drop — Dit is de standaardactie voor al het verkeer, zoals toegepast door de class-default die elke inspect-type policy-map beëindigt. Andere class-maps binnen een policy-map kunnen ook worden geconfigureerd om ongewenste verkeer te laten vallen. Het verkeer dat door de dalingsactie wordt behandeld wordt stil gelaten vallen (namelijk wordt geen bericht van de daling verzonden naar de relevante eind-gastheer) door ZFW, in tegenstelling tot een gedrag ACL wanneer het een "gastheer onbereikbaar"bericht ICMP naar de gastheer verzendt die het ontkende verkeer verzond. Op dit moment is er geen optie om het stille druppelgedrag te wijzigen. De logoptie kan met daling voor syslog bericht worden toegevoegd dat het verkeer door de firewall werd gelaten vallen.
- Pas - Deze actie staat de router toe om verkeer van één streek aan een andere door:sturen. De passactie volgt de status van verbindingen of sessies binnen het verkeer niet. Pas staat slechts het verkeer in één richting toe. Er moet een parallel beleid worden toegepast om

terugkeerverkeer in de tegenovergestelde richting te laten passeren. De pass actie is nuttig voor protocollen zoals IPSec ESP, IPSec AH, ISAKMP en andere inherent beveiligde protocollen met voorspelbaar gedrag. Het meeste toepassingsverkeer kan echter beter in de ZFW worden afgehandeld met de controleactie.

- Inspecteren — De inspectiemaatregel biedt op de staat gebaseerde verkeerscontrole. Als bijvoorbeeld het verkeer van de privézone naar de internetzone in het eerdere voorbeeldnetwerk wordt geïnspecteerd, onderhoudt de router verbinding- of sessieinformatie voor TCP- en User Datagram Protocol (UDP)-verkeer. Daarom laat de router terugkeerverkeer toe dat van internet-zone hosts wordt verzonden in antwoord op aanvragen van een privé-zone verbinding. Ook, kan inspecteren toepassingsinspectie en controle voor bepaalde dienstprotocollen verstrekken die kwetsbaar of gevoelig toepassingsverkeer kunnen dragen. Audit-trail kan worden toegepast met een parameter-kaart om verbinding/sessiestart, stop, duur, het overgedragen gegevensvolume en bron- en doeladressen op te nemen.

Acties worden geassocieerd met class-maps in policy-maps:

```
configure terminal
 policy-map type inspect z1-z2-pmap
  class type inspect service-cmap
   inspect|drop|allow [service-parameter-map]
```

Parameter-kaarten bieden opties om de verbindingsparameters voor een bepaald klasse-kaart inspectiebeleid te wijzigen.

Zone-Policy firewall-parameterkaarten configureren

Parameter-kaarten specificeren inspectiegedrag voor ZFW, voor parameters zoals DoS-bescherming, TCP-verbinding/UDP-sessietimers en instellingen voor audit-trailvastlegging. Parameter-kaarten worden ook toegepast met Layer 7-klasse en beleidskaarten om toepassingsspecifiek gedrag te definiëren, zoals HTTP-objecten, POP3- en IMAP-verificatievereisten en andere toepassingsspecifieke informatie.

Inspectie parameter-kaarten voor ZFW zijn geconfigureerd als type inspectie, vergelijkbaar met andere ZFW klasse en beleid-objecten:

```
stg-871-L(config)#parameter-map type inspect z1-z2-pmap stg-871-L(config-profile)#?
parameter-map commands:
  alert           Turn on/off alert
  audit-trail     Turn on/off audit trail
  dns-timeout     Specify timeout for DNS
  exit            Exit from parameter-map
  icmp            Config timeout values for icmp
  max-incomplete  Specify maximum number of incomplete connections before
                  clamping
  no              Negate or set default values of a command
  one-minute      Specify one-minute-sample watermarks for clamping
  sessions        Maximum number of inspect sessions
  tcp             Config timeout values for tcp connections
  udp             Config timeout values for udp flows
```

De specifieke types van parameter-kaarten specificeren parameters die door Layer 7 beleid van de toepassingsinspectie worden toegepast. Regex-type parameter-kaarten definiëren een reguliere expressie voor gebruik met HTTP-toepassingsinspectie die verkeer met een reguliere expressie filtert:

```
parameter-map type regex [parameter-map-name]
```

Protocol-info-type parameter-maps definiëren servernamen voor gebruik met IM Application inspection:

```
parameter-map type protocol-info [parameter-map-name]
```

De volledige configuratiedetails voor HTTP- en IM-toepassingsinspectie worden gegeven in de respectieve secties van de toepassingsinspectie van dit document.

Vastlegging toepassen voor op zone gebaseerd beleid en firewallbeleid

ZFW biedt registratieopties voor verkeer dat standaard wordt gedropt of geïnspecteerd of dat wordt geconfigureerd voor firewallbeleid. Audit-trail logboekregistratie is beschikbaar voor verkeer dat de ZFW inspecteert. Audit-trail wordt toegepast wanneer een audittrail wordt gedefinieerd in een parameter-kaart en de parameter-kaart met de inspectieactie wordt toegepast in een beleidskaart:

```
configure terminal
 policy-map type inspect z1-z2-pmap
  class type inspect service-cmap
   inspect|drop|allow [parameter-map-name (optional)]
```

Drop logging is beschikbaar voor verkeer dat de ZFW daalt. Drop logging is ingesteld door wanneer u een log toevoegt met de drop-actie in een policy-map:

```
configure terminal
 policy-map type inspect z1-z2-pmap
  class type inspect service-cmap
   inspect|drop|allow [service-parameter-map]
```

Zone-Policy Firewall, klasse-kaarten en beleidskaarten bewerken

ZFW bevat momenteel geen editor die de verschillende ZFW-structuren kan wijzigen, zoals policy-maps, class-maps en parameter-maps. Om overeenkomende verklaringen in een klasse-kaart of actietoepassing aan diverse klasse-kaarten in een beleid-kaart te herschikken, moet u deze stappen voltooien:

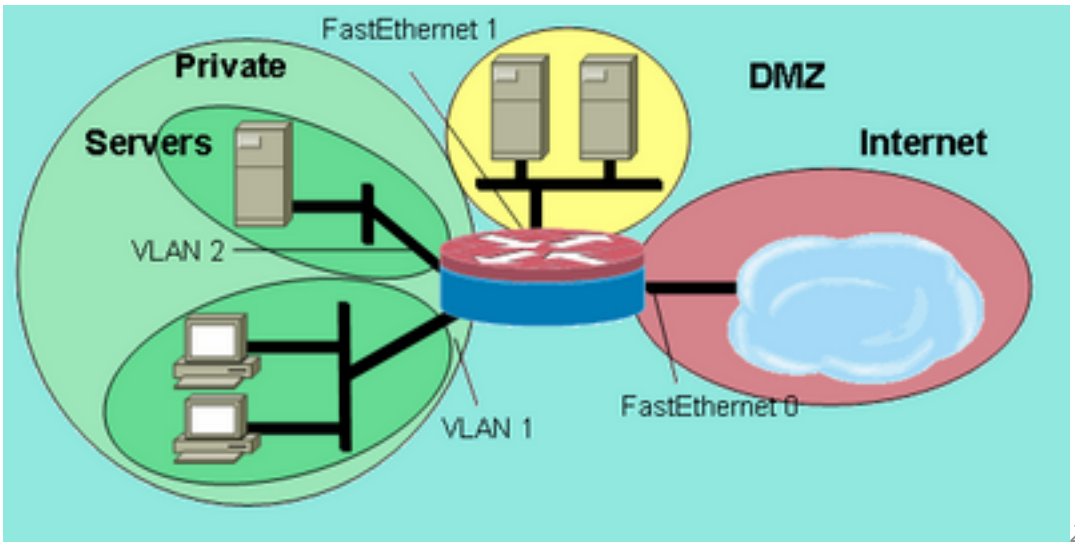
1. Kopieer de huidige structuur naar een teksteditor zoals Microsoft Windows Notepad of een editor zoals vi op Linux/Unix-platforms.
2. Verwijder de huidige structuur uit de routerconfiguratie.
3. Bewerk de structuur in de teksteditor.
4. Kopieer de structuur terug naar de router CLI.

Configuratievoorbeelden

Dit configuratievoorbeeld maakt gebruik van een Cisco 1811 geïntegreerde services router. Een basisconfiguratie met IP-connectiviteit, VLAN-configuratie en transparante overbrugging tussen twee particuliere Ethernet LAN-segmenten is beschikbaar in Bijlage A. De router wordt gescheiden in vijf zones:

- Het openbare internet is verbonden met Fast Ethernet 0 (internetzone)
- Twee internetservers zijn aangesloten op Fast Ethernet 1 (DMZ-zone)
- De Ethernet-switch is geconfigureerd met twee VLAN's:De werkstations zijn verbonden met VLAN1 (clientzone).De servers zijn verbonden met VLAN2 (serverzone).De client- en serverzones bevinden zich in hetzelfde subsysteem. Een transparante firewall wordt toegepast tussen de zones, zodat het interzone beleid op die twee interfaces alleen verkeer tussen de client- en serverzones kan beïnvloeden.
- De VLAN1- en VLAN2-interfaces communiceren met andere netwerken via de virtuele interface van de brug (BVI1). Deze interface wordt toegewezen aan de privé-zone. (Zie figuur 2.)

Afbeelding 2: Zone-topologiedetail

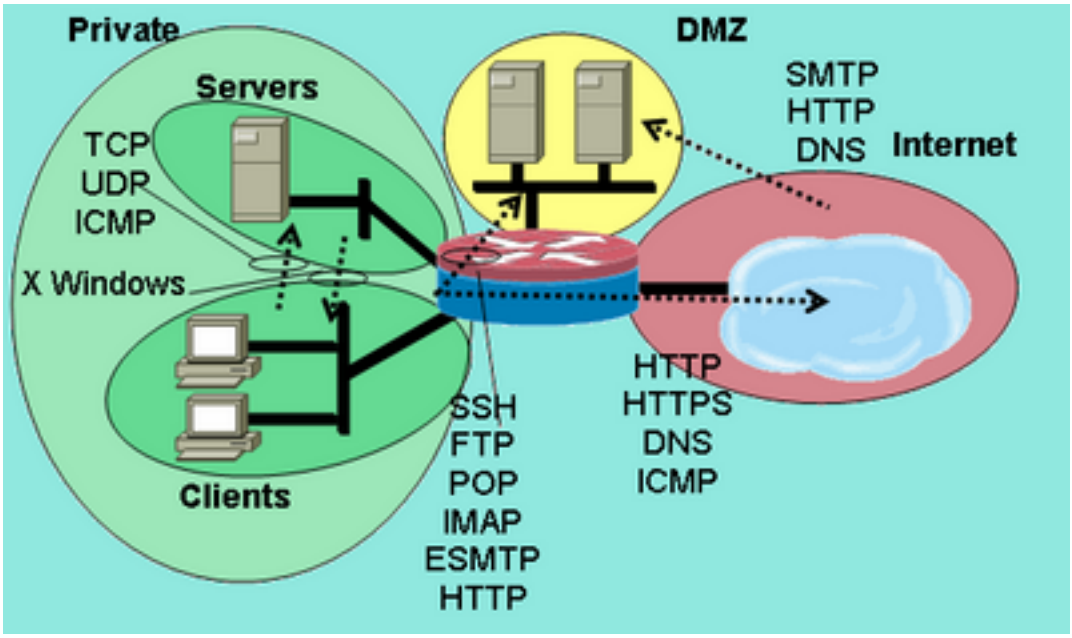


Zone-topologiedetail

Dit beleid wordt toegepast, waarbij de netwerkzones eerder zijn gedefinieerd:

- Hosts in de internetzone kunnen DNS-, SMTP- en SSH-services bereiken op één server in de DMZ. De andere server biedt SMTP-, HTTP- en HTTPS-services. Het firewallbeleid beperkt toegang tot de specifieke diensten die op elke host beschikbaar zijn.
- De DMZ-hosts kunnen geen verbinding maken met hosts in een andere zone.
- Hosts in de clientzone kunnen verbinding maken met hosts in de serverzone op alle TCP-, UDP- en ICMP-services.
- Hosts in de serverzone kunnen geen verbinding maken met hosts in de clientzone, behalve dat een op UNIX gebaseerde toepassingsserver X Windows-clientsessies kan openen naar X Windows-servers op desktop-pc's in de clientzone op poorten 6900 tot 6910.
- Alle hosts in de privézone (combinatie van clients en servers) kunnen toegang krijgen tot hosts in de DMZ op SSH-, FTP-, POP-, IMAP-, ESMTP- en HTTP-services en in de internetzone op HTTP-, HTTPS- en DNS-services en ICMP. Bovendien wordt de applicatie-inspectie toegepast op HTTP-verbindingen van de privézone naar de internetzone om te garanderen dat ondersteunde IM- en P2P-toepassingen niet worden uitgevoerd op poort 80 (zie afbeelding 3).

Afbeelding 3: Toepassingsrechten voor Zone-pair-services die in het configuratievoorbeeld moeten worden toegepast



Toepassingsrechten voor Zone-pair-services die in het configuratievoorbeeld moeten worden toegepast

Dit firewallbeleid wordt geconfigureerd in volgorde van complexiteit:

1. Clients-servers, TCP/UDP/ICMP-inspectie
2. Private-DMZ SSH/FTP/POP/IMAP/ESMTP/HTTP-inspectie
3. Internet -DMZ SMTP/HTTP/DNS-inspectie beperkt door hostadres
4. Servers-Clients X Windows-inspectie met een poortapplicatie-mapping (PAM)-gespecificeerde service
5. Private-Internet HTTP/HTTPS/DNS/ICMP met HTTP-toepassingsinspectie

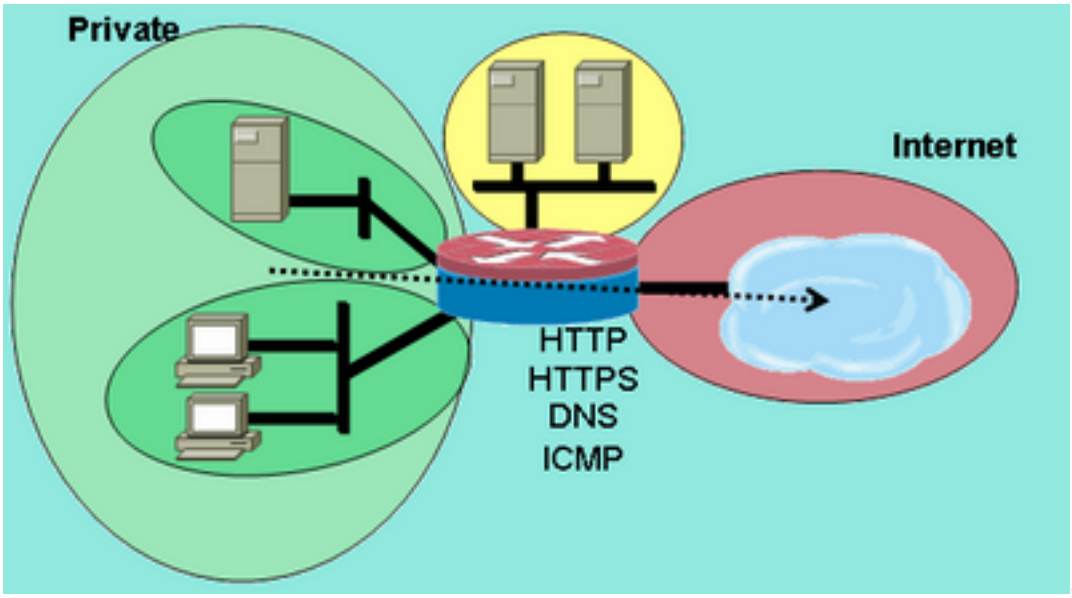
Omdat u delen van de configuratie op verschillende netwerksegmenten op verschillende tijden toepast, is het belangrijk om te onthouden dat een netwerksegment connectiviteit aan andere segmenten verliest wanneer het in een zone wordt geplaatst. Bijvoorbeeld, wanneer de privé zone wordt gevormd, verliezen de gastheren in de privé-zone connectiviteit aan de DMZ en de streken van Internet tot hun respectieve beleid wordt bepaald.

Firewall voor stateful inspection routing

Privé-internetbeleid configureren

Figuur 4 illustreert de configuratie van privé internetbeleid.

Afbeelding 4: Serviceinspectie van Private Zone naar Internet Zone



Serviceinspectie van Private Zone naar Internet Zone

Het privé internetbeleid past Layer 4-inspectie toe op HTTP, HTTPS, DNS en Layer 4-inspectie voor ICMP van de private zone naar de internetzone. Dit staat verbindingen van de privé streek aan de streek van Internet toe en staat het terugkeerverkeer toe. Layer 7-inspectie biedt de voordelen van een striktere toepassingscontrole, betere beveiliging en ondersteuning voor toepassingen die een oplossing vereisen. Layer 7-inspectie, zoals vermeld, vereist echter een beter begrip van netwerkactiviteit, aangezien Layer 7-protocollen die niet voor inspectie zijn geconfigureerd niet tussen zones zijn toegestaan.

1. Definieer class-maps die het verkeer beschrijven dat u wilt toestaan tussen zones, gebaseerd op het eerder beschreven beleid:
```
configure terminal
 class-map type inspect match-any internet-traffic-class
  match protocol http
  match protocol https
  match protocol dns
  match protocol icmp
```
2. Configureer een policy-map om verkeer op de class-maps te inspecteren die u zojuist hebt gedefinieerd:
```
configure terminal
 policy-map type inspect private-internet-policy
  class type inspect internet-traffic-class
   inspect
```
3. Configureer de privé- en internetzones en wijs routerinterfaces toe aan hun respectievelijke zones:
```
configure terminal
 zone security private
 zone security internet
 int bvi1
  zone-member security private
 int fastethernet 0
  zone-member security internet
```

Configureer de zone-pair en pas de juiste policy-map toe.

> **Opmerking:** U hoeft momenteel alleen het privaat internetzonepaar te configureren om verbindingen te inspecteren die zijn opgenomen in de privézone die naar de internetzone reist, zoals hieronder weergegeven:

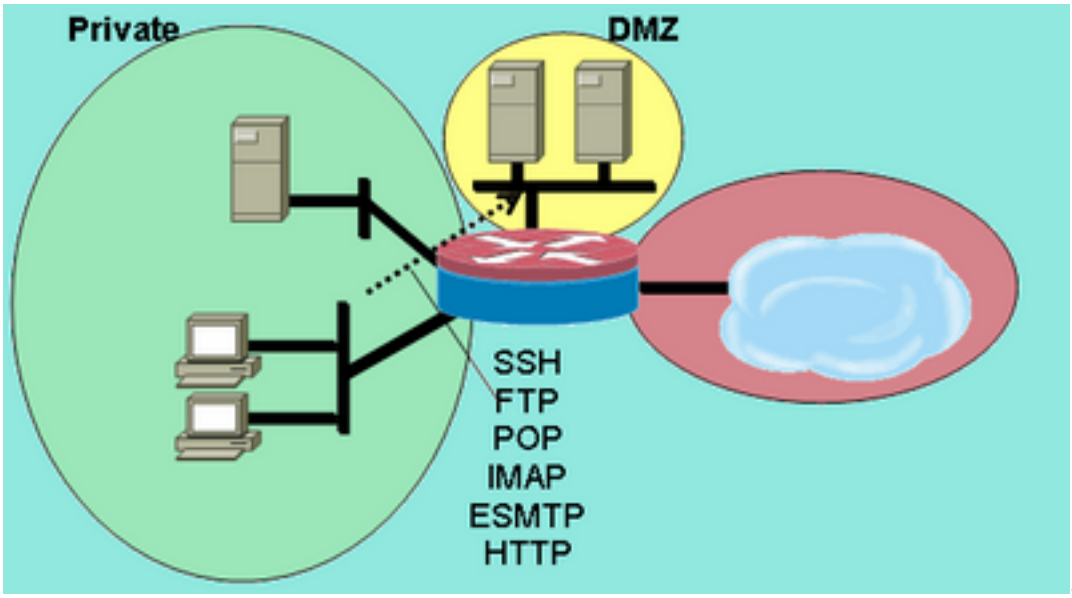
```
configure terminal
 zone-pair security private-internet source private destination internet
  service-policy type inspect private-internet-policy
```

Dit voltooit de configuratie van Layer 7-inspectiebeleid op het privaat internet-zone-paar om HTTP-, HTTPS-, DNS- en ICMP-verbindingen van de clientzone naar de serverzone toe te staan en toepassingsinspectie op HTTP-verkeer toe te passen om ervoor te zorgen dat ongewenst verkeer geen TCP 80, HTTP-servicepoort kan doorgeven.

Private DMZ-beleid configureren

Figuur 5 illustreert de configuratie van privé beleid DMZ.

Afbeelding 5: Service Inspection van Private Zone naar DMZ Zone



Service Inspection van Private Zone naar DMZ Zone

Het privé DMZ beleid voegt complexiteit toe omdat het een beter begrip van het netwerkverkeer tussen streken vereist. Dit beleid past Layer 7-inspectie toe vanaf de private zone op de DMZ. Dit staat verbindingen van de privé streek aan DMZ toe en staat het terugkeerverkeer toe. Layer 7-inspectie biedt de voordelen van een striktere toepassingscontrole, betere beveiliging en ondersteuning voor toepassingen die een oplossing vereisen. Layer 7-inspectie, zoals vermeld, vereist echter een beter begrip van netwerkactiviteit, aangezien Layer 7-protocollen die niet voor inspectie zijn geconfigureerd niet tussen zones zijn toegestaan.

1. Definieer class-maps die het verkeer beschrijven dat u wilt toestaan tussen zones, gebaseerd op het eerder beschreven beleid:
   ```
   configure terminal
    class-map type inspect match-any L7-inspect-class
     match protocol ssh
     match protocol ftp
     match protocol pop
     match protocol imap
     match protocol esmtp
     match protocol http
   ```
2. Configureer beleid-kaarten om verkeer op de klasse-kaarten te inspecteren u net bepaalde:
   ```
   configure terminal
    policy-map type inspect private-dmz-policy
     class type inspect L7-inspect-class
   ```

```
  inspect
```

3. Configureer de privé- en DMZ-zones en wijs routerinterfaces toe aan hun respectievelijke zones:

```
configure terminal
 zone security private
 zone security dmz
 int bvi1
  zone-member security private
 int fastethernet 1
  zone-member security dmz
```

4. Configureer de zone-pair en pas de juiste policy-map toe.

Opmerking: U hoeft op dit moment alleen het privé-DMZ-zonepaar te configureren om verbindingen te inspecteren die zijn afkomstig uit de private zone die naar de DMZ reist, zoals hieronder weergegeven:

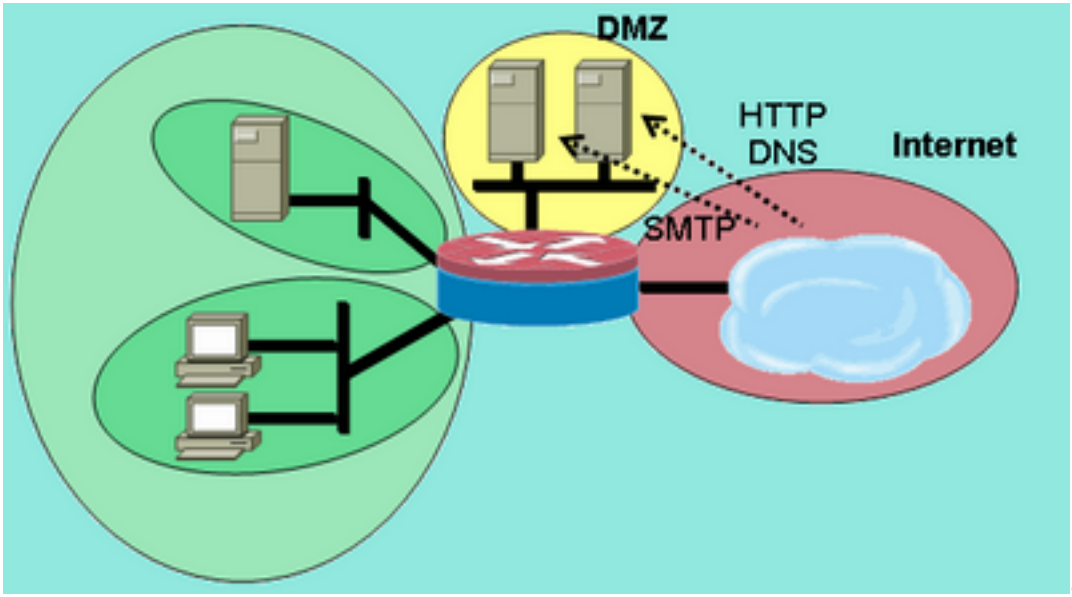
```
configure terminal
 zone-pair security private-dmz source private destination dmz
  service-policy type inspect private-dmz-policy
```

Hiermee is de configuratie van Layer 7-inspectiebeleid op de private DMZ voltooid om alle TCP-, UDP- en ICMP-verbindingen van de clientzone naar de serverzone toe te staan. Het beleid past geen correctie toe voor ondergeschikte kanalen, maar biedt een voorbeeld van eenvoudig beleid om de meeste toepassingsverbindingen aan te passen.

Internet DMZ-beleid configureren

Figuur 6 illustreert de configuratie van Internet DMZ beleid.

Afbeelding 6: Servicecontrole van Internet Zone naar DMZ Zone



Servicecontrole van Internet Zone naar DMZ Zone

Dit beleid past Layer 7-inspectie toe vanaf de internetzone op de DMZ. Dit staat verbindingen van de zone van Internet aan DMZ toe en staat het terugkeerverkeer van de gastheren DMZ aan de gastheren van Internet toe die de verbinding voortkwamen. Het Internet DMZ-beleid combineert Layer 7-inspectie met adresgroepen die door ACL's zijn gedefinieerd om de toegang tot specifieke services op specifieke hosts, groepen hosts of subnetten te beperken. Om dit te verwezenlijken nesten een klasse-kaart die de diensten binnen een andere klasse-kaart specificeert die

verwijzingen een ACL om IP adressen te specificeren.

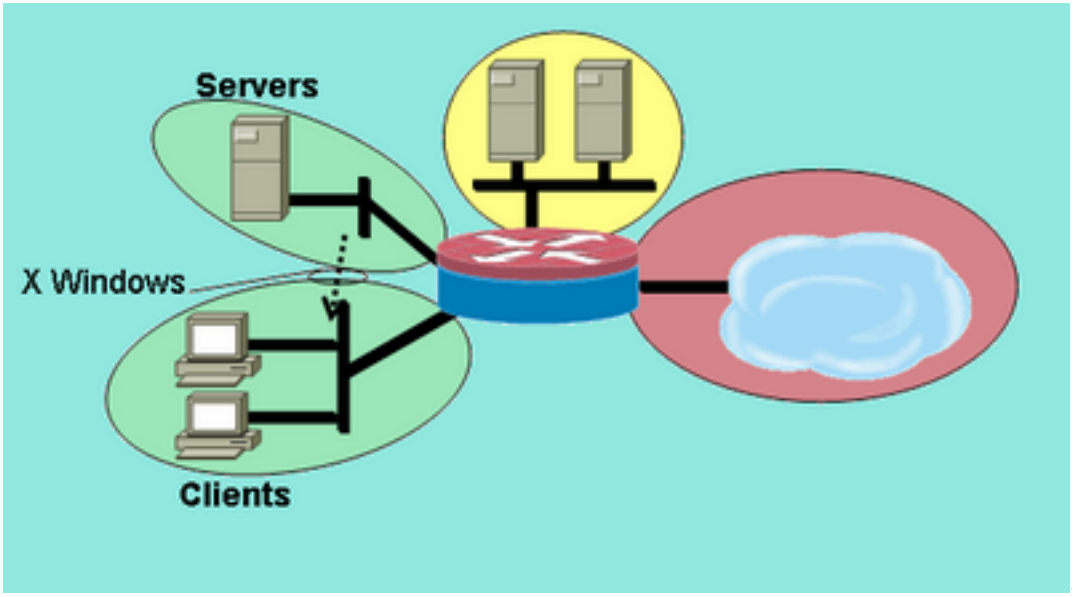
1. Definieer class-maps en ACL's die het verkeer beschrijven dat u wilt toestaan tussen zones, gebaseerd op het eerder beschreven beleid.Er moeten meerdere class-maps voor services worden gebruikt, aangezien er verschillende toegangsbeleidsregels worden toegepast voor toegang tot twee verschillende servers. Internethosts zijn toegestaan DNS- en HTTP-verbindingen naar 172.16.2.2 en SMTP-verbindingen zijn toegestaan naar 172.16.2.3. Let op het verschil in de class-maps. De klasse-kaarten die de diensten specificeren gebruiken het gelijke-om het even welk sleutelwoord om het even welke vermelde diensten toe te staan. De klasse-kaarten die ACL's met de serviceklasse-kaarten associëren, gebruiken het trefwoord match-all om te vereisen dat aan beide voorwaarden in de klassenkaart moet worden voldaan om verkeer toe te staan:
```
configure terminal
 access-list 110 permit ip any host 172.16.2.2
 access-list 111 permit ip any host 172.16.2.3
 class-map type inspect match-any dns-http-class
  match protocol dns
  match protocol http
 class-map type inspect match-any smtp-class
  match protocol smtp
 class-map type inspect match-all dns-http-acl-class
  match access-group 110
  match class-map dns-http-class
 class-map type inspect match-all smtp-acl-class
  match access-group 111
  match class-map smtp-class
```
2. Configureer beleid-kaarten om verkeer op de klasse-kaarten te inspecteren u net bepaalde:
```
configure terminal
 policy-map type inspect internet-dmz-policy
  class type inspect dns-http-acl-class
   inspect
  class type inspect smtp-acl-class
   inspect
```
3. Configureer de internet- en DMZ-zones en wijs routerinterfaces toe aan hun respectievelijke zones. Sla de DMZ-configuratie over als u deze in de vorige sectie hebt ingesteld:
```
configure terminal
zone security internet
zone security dmz
int fastethernet 0
 zone-member security internet
int fastethernet 1
 zone-member security dmz
```
4. Configureer de zone-pair en pas de juiste policy-map toe.**Opmerking:** U hoeft momenteel alleen het internet DMZ-zonepaar te configureren, om verbindingen te inspecteren die afkomstig zijn uit de internetzone die naar de DMZ-zone reist, zoals hieronder weergegeven:
```
configure terminal
 zone-pair security internet-dmz source internet destination dmz
  service-policy type inspect internet-dmz-policy
```
Dit voltooit de configuratie van het adrespecifieke Layer 7-inspectiebeleid op het internet DMZ-zone-paar.

Transparante firewall voor stateful inspection

Beleid voor servers/clients configureren

Dit volgende cijfer illustreert de configuratie van server-client beleid.

Afbeelding 7: Servicecontrole van serverzone naar clientzone



Servicecontrole van serverzone naar clientzone

Het server-clients beleid past inspectie toe met een door de gebruiker gedefinieerde service. Layer 7-inspectie wordt toegepast vanaf de serverzone op de clientzone. Dit maakt X Windows verbindingen met een specifieke poortbereik van de serverzone tot de clientzone mogelijk en laat het retourverkeer toe. X Windows is geen native-ondersteund protocol in PAM, zodat een door de gebruiker geconfigureerde service in PAM moet worden gedefinieerd zodat de ZFW het juiste verkeer kan herkennen en inspecteren.

Twee of meer routerinterfaces zijn in een IEEE-bridge-groep geconfigureerd om geïntegreerde routing en bridging (IRB) te bieden voor overbrugging tussen de interfaces in de bridge-groep en voor routing naar andere subnetten via de virtuele interface van de bridge (BVI). Het transparante firewallbeleid past firewallinspectie voor verkeer toe "dat de brug"oversteekt, maar niet voor verkeer dat de brug-groep via BVI verlaat. Het inspectiebeleid is alleen van toepassing op verkeer dat de bruggroep oversteekt. Daarom in dit scenario, wordt de inspectie slechts toegepast op verkeer dat zich tussen de cliënten en de serverzones beweegt, die binnen de privé zone worden genesteld. Het beleid dat wordt toegepast tussen de privézone, de openbare zone en de DMZ-zone, komt alleen in werking als het verkeer de bruggroep verlaat via de BVI. Wanneer het verkeer via de BVI vertrekt vanuit de client- of serverzones, wordt het transparante firewallbeleid niet aangeroepen.

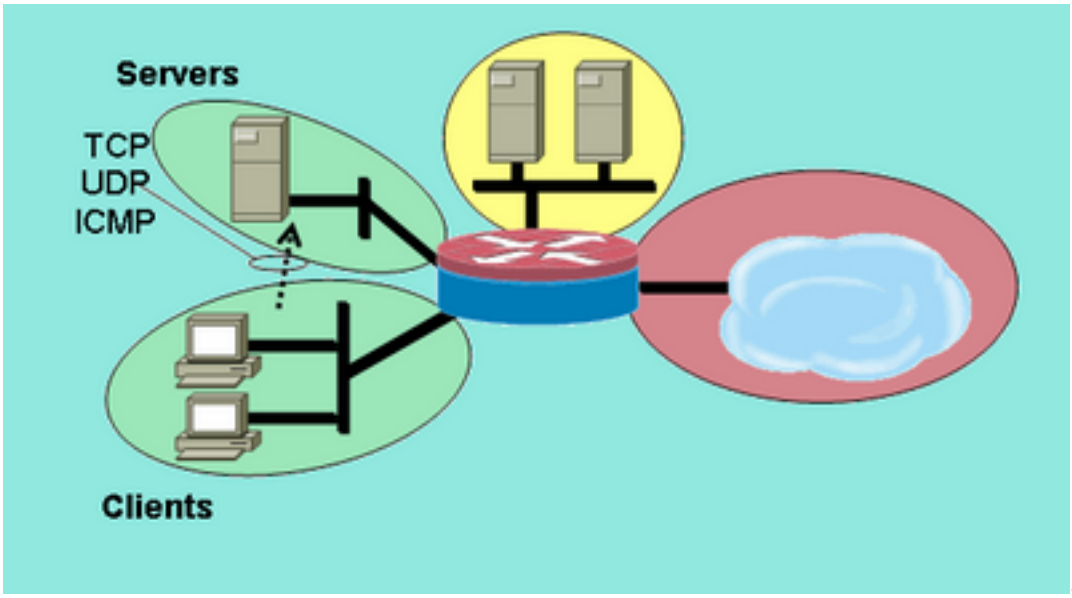
1. Configureer PAM met een door de gebruiker gedefinieerde ingang voor X Windows.X Windows-clients (waar toepassingen worden gehost) open verbindingen voor weergave informatie aan clients (waar de gebruiker werkt) in een bereik dat begint bij poort 6900.Elke extra verbinding gebruikt opeenvolgende poorten, dus als een client 10 verschillende sessies op één host weergeeft, gebruikt de server poorten 6900-6909. Daarom als u het poortbereik van 6900 tot 6909 inspecteert, mislukken verbindingen die zijn geopend naar poorten na 6909:
```
configure terminal
 ip port-map user-Xwindows port tcp from 6900 to 6910
```
2. Bekijk PAM-documenten om extra PAM-vragen te beantwoorden of controleer de documentatie van de gedetailleerde protocolinspectie voor informatie over de details van interoperabiliteit tussen PAM en Cisco IOS firewall-stateful inspection.

3. Definieer class-maps die het verkeer beschrijven dat u wilt toestaan tussen zones, gebaseerd op het eerder beschreven beleid:
```
configure terminal
 class-map type inspect match-any Xwindows-class
  match protocol user-Xwindows
```
4. Configureer beleid-kaarten om verkeer op de klasse-kaarten te inspecteren u net bepaalde:
```
configure terminal
 policy-map type inspect servers-clients-policy
  class type inspect Xwindows-class
   inspect
```
5. Configureer de client- en serverzones en wijs routerinterfaces toe aan hun respectievelijke zones.Als u deze zones en toegewezen interfaces in de sectie Clients-Servers Policy Configuration hebt geconfigureerd, kunt u overslaan naar de zone-paardefinitie. Voor de volledigheid wordt overbrugging van de IRB-configuratie verstrekt:
```
configure terminal
bridge irb
bridge 1 protocol ieee
bridge 1 route ip
zone security clients
zone security servers
 int vlan 1
 bridge-group 1
 zone-member security clients
int vlan 2
 bridge-group 1
 zone-member security servers
```
6. Configureer de zone-pair en pas de juiste policy-map toe.**Opmerking:** U hoeft momenteel alleen het zone-paar van de servers-clients te configureren om de verbindingen te inspecteren die zijn afgeleid uit de serverzone die naar de clientzone reist, zoals hieronder getoond:
```
configure terminal
 zone-pair security servers-clients source servers destination clients
  service-policy type inspect servers-clients-policy
```
Hiermee is de configuratie van het door de gebruiker gedefinieerde inspectiebeleid in het zone-paar van de servers-clients voltooid, zodat X Windows-verbindingen van de serverzone naar de clientzone mogelijk zijn.

Beleid voor clientservers configureren

Afbeelding 8 illustreert de configuratie van het clientserverbeleid.

Afbeelding 8: Servicecontrole van clientzone naar serverzone



Servicecontrole van clientzone naar serverzone

Het client-servers beleid is minder complex dan de anderen. Layer 4-inspectie wordt toegepast vanaf de clientzone op de serverzone. Dit maakt verbindingen mogelijk van de clientzone naar de serverzone en geeft verkeer terug. Layer 4-inspectie biedt het voordeel van eenvoud in de firewallconfiguratie, in die zin dat er slechts een paar regels nodig zijn om het meeste toepassingsverkeer toe te staan. Layer 4-inspectie heeft echter ook twee grote nadelen:

- Toepassingen zoals FTP of mediadiensten onderhandelen vaak over een extra ondergeschikt kanaal van de server naar de client. Deze functionaliteit wordt meestal ondergebracht in een service fix-up die het dialoogvenster controlekanaal bewaakt en het ondergeschikte kanaal toestaat. Deze mogelijkheid is niet beschikbaar in Layer 4-inspectie.
- Layer 4-inspectie maakt bijna al het verkeer op de toepassingslaag mogelijk. Als het netwerkgebruik moet worden gecontroleerd zodat slechts een paar toepassingen door de firewall worden toegestaan, moet ACL op uitgaand verkeer worden gevormd om de diensten te beperken die door de firewall worden toegestaan.

Beide routerinterfaces worden geconfigureerd in een IEEE-bruggroep, zodat dit firewallbeleid transparante firewallinspectie toepast. Dit beleid wordt toegepast op twee interfaces in een IEEE IP-bruggroep. Het inspectiebeleid is alleen van toepassing op verkeer dat de bruggroep kruist. Dit verklaart waarom de cliënten en de serverzones binnen de privé-zone worden genesteld.

1. Definieer class-maps die het verkeer beschrijven dat u wilt toestaan tussen zones, gebaseerd op het eerder beschreven beleid:
```
configure terminal
 class-map type inspect match-any L4-inspect-class
 match protocol tcp
 match protocol udp
 match protocol icmp
```
2. Configureer beleid-kaarten om verkeer op de klasse-kaarten te inspecteren u net bepaalde:
```
configure terminal
 policy-map type inspect clients-servers-policy
 class type inspect L4-inspect-class
  inspect
```
3. Configureer de clients en servers zones en wijs routerinterfaces toe aan hun respectievelijke zones:
```
configure terminal
 zone security clients
 zone security servers
```

```
interface vlan 1
 zone-member security clients
interface vlan 2
 zone-member security servers
```

4. Configureer de zone-pair en pas de juiste policy-map toe.**Opmerking:** U hoeft momenteel alleen het zone-paar van de clients-servers te configureren, om verbindingen te inspecteren die zijn gesourcet in de clientzone die naar de serverzone reist, zoals hieronder getoond:
```
configure terminal
 zone-pair security clients-servers source clients destination servers
  service-policy type inspect clients-servers-policy
```
Hiermee is de configuratie van Layer 4-inspectiebeleid voor het zone-paar van de clientservers voltooid, zodat alle TCP-, UDP- en ICMP-verbindingen van de clientzone naar de serverzone mogelijk zijn. Het beleid is niet van toepassing fixup voor ondergeschikte kanalen maar biedt een voorbeeld van eenvoudig beleid om de meeste toepassingsverbindingen aan te passen.

Rate Policy voor zone-gebaseerde beleidsfirewall

Gegevensnetwerken profiteren vaak van de mogelijkheid om het transmissietarief van specifieke soorten netwerkverkeer te beperken en de impact van verkeer met een lagere prioriteit te beperken tot meer zaken-essentieel verkeer. Cisco IOS-software biedt deze mogelijkheid met traffic policing (verkeerspolitie), die de nominale snelheid en burst van het verkeer beperkt. Cisco IOS-software ondersteunt traffic policing sinds Cisco IOS-softwarerelease 12.1(5)T.

Cisco IOS-softwarerelease 12.4(9)T verbetert ZFW met snelheidsbeperking wanneer u de mogelijkheid toevoegt om verkeer te controleren dat overeenkomt met de definities van een specifieke klasse-kaart wanneer de firewall van de ene naar de andere veiligheidszone wordt gepasseerd. Dit biedt het gemak van één configuratiepunt om specifiek verkeer te beschrijven, firewallbeleid toe te passen, en politie dat de consumptie van de verkeersbandbreedte. ZFW verschilt van interface-based in die zin dat het alleen de acties overbrengt voor beleidsconformiteit en drop voor beleidsschending. ZFW kan geen verkeer voor DSCP markeren.

ZFW kan alleen bandbreedtegebruik in bytes/seconde, pakket/seconde en bandbreedtepercentage worden niet aangeboden specificeren. ZFW kan met of zonder interface-based worden toegepast. Daarom als extra mogelijkheden worden vereist, kunnen deze eigenschappen door interface-based worden toegepast. Als de interface-based wordt gebruikt in combinatie met een firewall, zorg er dan voor dat het beleid niet conflicteert.

ZFW-beleid configureren

ZFW-toezicht beperkt verkeer in een policy-map class-map tot een door de gebruiker gedefinieerde snelheidswaarde tussen 8.000 en 2.000.000.000 bits per seconde, met een configureerbare burstwaarde binnen het bereik van 1.000 tot 512.000.000 bytes.

ZFW-toezicht wordt geconfigureerd via een extra configuratielijn in de beleidskaart, die wordt toegepast na de beleidsactie:

```
policy-map type inspect private-allowed-policy
 class type inspect http-class
  inspect
  police rate [bps rate value <8000-2000000000>] burst [value in bytes <1000-512000000>]
```

Sessiebeheer

ZFW-beleid introduceerde ook sessiecontrole om de sessietelling voor verkeer te beperken in een beleidskaart die van toepassing is en overeenkomt met een klasse-map. Dit maakt het mogelijk om het Dos-beschermingsbeleid per klasse-map toe te passen. Effectief, dit staat granulaire controle op het aantal sessies toe die van toepassing is dat aanpast om het even welke bepaalde klasse-kaart die een streek-paar kruist. Als dezelfde class-map wordt gebruikt op meerdere policy-maps of zone-paren, kunnen verschillende sessielimieten worden toegepast op de verschillende class-map applicaties.

Session control wordt toegepast wanneer een parameter-map is geconfigureerd die het gewenste sessievolume bevat, dan wordt de parameter-map toegevoegd aan de inspectieactie die is toegepast op een klasse-map onder een policy-map:

```
parameter-map type inspect my-parameters
 sessions maximum [1-2147483647]

policy-map type inspect private-allowed-policy
 class type inspect http-class
  inspect my-parameters
```

Parameter-kaarten kunnen alleen worden toegepast op de inspect actie en zijn niet beschikbaar op pas of drop acties.

ZFW-sessiecontrole- en -politieactiviteiten zijn zichtbaar met deze opdracht:

```
show policy-map type inspect zone-pair
```

Toepassingsinspectie

Toepassingsinspectie biedt ZFW extra mogelijkheden. Het beleid van de toepassingsinspectie wordt toegepast bij Layer 7 van het OSI model, waar de gebruikerstoepassingen berichten verzenden en ontvangen die de toepassingen toestaan om nuttige mogelijkheden aan te bieden. Sommige toepassingen kunnen ongewenste of kwetsbare mogelijkheden bieden, zodat de berichten die aan deze mogelijkheden zijn gekoppeld, moeten worden gefilterd om activiteiten op de toepassingsservices te beperken.

Cisco IOS-softwarerelease ZFW biedt toepassingsinspectie en -controle op deze toepassingsservices:

- HTTP
- SMTP
- POP3
- IMAP
- Sun RPC
- P2P-toepassingsverkeer
- IM-toepassingen

Toepassingsinspectie en -controle (AIC) varieert in capaciteit per dienst. HTTP-inspectie biedt granulaire filtering op verschillende soorten toepassingsactiviteit en biedt mogelijkheden om de overdrachtgrootte, de lengte van webadressen en browseractiviteit te beperken om naleving van toepassingsgedragsnormen af te dwingen en soorten inhoud te beperken die via de service

worden overgedragen. AIC voor SMTP kan inhoudslengte beperken en protocolnaleving afdwingen. POP3- en IMAP-inspectie kunnen ervoor zorgen dat gebruikers beveiligde verificatiemechanismen gebruiken om te voorkomen dat er problemen met gebruikersreferenties ontstaan.

Toepassingsinspectie is ingesteld als een extra set van applicatiespecifieke klassekaarten en beleidskaarten, die vervolgens worden toegepast op de huidige inspectie klassekaarten en beleidskaarten door het bepalen van het toepassingsservicebeleid in de inspectie beleid-kaart.

HTTP-toepassingsinspectie

Toepassingsinspectie kan worden toegepast op HTTP-verkeer om ongewenst gebruik van HTTP-servicepoort te controleren voor andere toepassingen zoals IM, P2P-bestandsdeling en tunneltoepassingen die andere firewalltoepassingen kunnen omleiden via TCP 80.

Configureer een klasse-kaart van toepassingsinspectie om verkeer te beschrijven dat toegestaan HTTP-verkeer schendt:

```
! configure the actions that are not permitted
class-map type inspect http match-any http-aic-cmap
 match request port-misuse any
 match req-resp protocol-violation
! define actions to be applied to unwanted traffic
policy-map type inspect http http-aic-pmap
 class type insp http http-aic-cmap
  reset
  log
! define class-map for stateful http inspection
class-map type inspect match-any http-cmap
 match protocol http
! define class-map for stateful inspection for other traffic
class-map type inspect match-any other-traffic-cmap
 match protocol smtp
 match protocol dns
 match protocol ftp
! define policy-map, associate class-maps and actions
policy-map type inspect priv-pub-pmap
 class type inspect http-cmap
  inspect
  service-policy http http-aic-pmap
 class type inspect other-traffic-cmap
  inspect
```

HTTP-toepassingsinspectie - verbeteringen

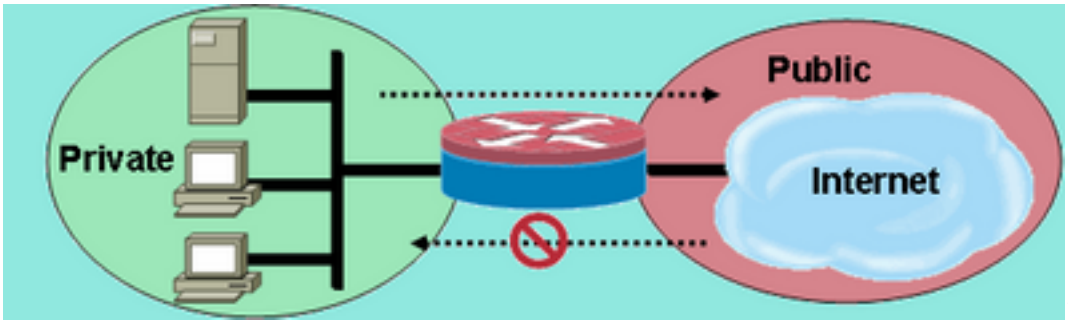
Cisco IOS-softwarerelease 12.4(9)T introduceert verbeteringen in ZFW HTTP-inspectiemogelijkheden. Cisco IOS Firewall introduceerde HTTP-toepassingsinspectie in Cisco IOS-softwarerelease 12.3(14)T. Cisco IOS-softwarerelease 12.4(9)T vergroot de huidige mogelijkheden wanneer u toevoegt:

- Mogelijk om verzoeken en antwoorden toe te staan, te weigeren en te bewaken op basis van de naam van de kop en de headerwaarden. Dit is handig om verzoeken en antwoorden te blokkeren die kwetsbare headervelden dragen.
- Mogelijkheid om de grootte van verschillende elementen in de HTTP-aanvraag en reactiekoppen te beperken zoals maximale URL-lengte, maximale header-lengte, maximaal

aantal headers, maximale header-line lengte, enzovoort. Dit is handig om bufferoverloop te voorkomen.
- Mogelijkheid om verzoeken en antwoorden te blokkeren die meerdere kopregels van hetzelfde type bevatten; Bijvoorbeeld, een verzoek met twee content-length headers.
- Mogelijkheid om verzoeken en antwoorden te blokkeren met niet-ASCII-headers. Dit is nuttig om verschillende aanvallen te voorkomen die binaire en andere niet-ASCII tekens gebruiken om wormen en andere schadelijke inhoud aan webservers te leveren.
- De mogelijkheid om HTTP-methoden in door de gebruiker opgegeven categorieën te groeperen en de flexibiliteit om elk van de groepen te blokkeren/toestaan/bewaken, wordt aangeboden. HTTP RFC staat een beperkte set HTTP-methoden toe. Sommige standaardmethoden worden als onveilig beschouwd omdat ze kunnen worden gebruikt om kwetsbaarheden op een webserver te exploiteren. Veel van de niet-standaard methoden hebben een slecht beveiligingsrecord.
- Methode om specifieke URI's te blokkeren op basis van een door de gebruiker ingestelde reguliere expressie. Deze functie geeft een gebruiker de mogelijkheid om aangepaste URI en queries te blokkeren.
- Mogelijkheid om spof header types (vooral server header type) met aangepaste strings. Dit is nuttig in een geval waar een aanvaller de reacties van de webserver analyseert en zoveel mogelijk informatie leert, dan lanceert een aanval die zwakheden in die bepaalde webserver exploiteert.
- Mogelijk om een waarschuwing te blokkeren of uit te geven op een HTTP-verbinding als een of meer HTTP-parameterwaarden overeenkomen met waarden die door de gebruiker als reguliere expressie zijn ingevoerd. Enkele van de mogelijke HTTP-waardecontexten zijn header, body, gebruikersnaam, wachtwoord, gebruikersagent, aanvraagregel, statusregel en gedecodeerde CGI-variabelen.

De voorbeelden van de configuratie voor de verbeteringen van de toepassingsinspectie van HTTP veronderstellen een eenvoudig netwerk, dat in Figuur 9 wordt getoond.

Afbeelding 9: Toepassingsinspectie uitgaande van een eenvoudig netwerk



Toepassingsinspectie uitgaande van een eenvoudig netwerk

De firewall groepeert verkeer in twee klassen:

- HTTP-verkeer
- Alle andere single-channel TCP-, UDP- en ICMP-verkeer

HTTP is gescheiden om specifieke inspectie van webverkeer mogelijk te maken. Hiermee kunt u toezicht configureren in de eerste sectie van dit document en HTTP-toepassingsinspectie in de tweede sectie. U kunt specifieke class-maps en policy-maps configureren voor P2P- en IM-verkeer in de derde sectie van dit document. Connectiviteit is toegestaan van de privézone naar de openbare zone. Van de openbare zone naar de privézone wordt geen verbinding tot stand gebracht.

Raadpleeg Bijlage C voor een volledige configuratie waarin het initiële beleid wordt geïmplementeerd.

Verbeteringen in HTTP-toepassingsinspectie configureren

HTTP-toepassingsinspectie (en ander beleid voor toepassingsinspectie) vereist een complexere configuratie dan de basisconfiguratie van Layer 4. U moet Layer 7-verkeersclassificatie en -beleid configureren om specifiek verkeer te herkennen dat u wilt besturen en om de gewenste actie toe te passen op gewenst en ongewenst verkeer.

HTTP-toepassingsinspectie (vergelijkbaar met andere soorten toepassingsinspectie) kan alleen worden toegepast op HTTP-verkeer. Aldus, moet u Layer 7 class-maps en policy-maps voor specifiek HTTP-verkeer definiëren, vervolgens een Layer-4 class-map specifiek voor HTTP definiëren en Layer-7-beleid toepassen op HTTP-inspectie in een Layer-4 policy-map, als zodanig:

```
!configure the layer-7 traffic characteristics:
class-map type inspect http match-any http-l7-cmap
 match  req-resp protocol-violation
 match  request body length gt 4096
!
!configure the action to be applied to the traffic
!matching the specific characteristics:
policy-map type inspect http http-l7-pmap
 class type inspect http http-l7-cmap
  reset
  log
!
!define the layer-4 inspection policy
class-map type inspect match-all http-l4-cmap
 match protocol http
!
!associate layer-4 class and layer-7 policy-map
!in the layer-4 policy-map:
policy-map type inspect private-allowed-policy
 class type inspect http-l4-cmap
  inspect
  service-policy http http-l7-pmap
```

Al deze verkeerskenmerken van HTTP-toepassingsinspectie worden gedefinieerd in een Layer 7-klasse-kaart:

- De opdracht voor headerinspectie biedt de mogelijkheid om verzoeken of antwoorden waarvan de header overeenkomt met de geconfigureerde reguliere expressie toe te staan/te weigeren/te monitoren. Sta toe of stel actie terug kan worden toegepast op een verzoek of een reactie die de klasse-kaart criteria aanpassen. Toevoeging van de logactie veroorzaakt een syslog bericht:
  `APPFW-6-HTTP_HDR_REGEX_MATCHED`
  Opdrachtgebruik:

```
match {request|response|req-resp} header regex <parameter-map-name>
```

Voorbeeld van gebruikscase

- Configureer een http appfw-beleid om verzoek of antwoord te blokkeren waarvan de header niet-ASCII-tekens bevat.

```
parameter-map type regex non_ascii_regex
   pattern “[^\x00-\x80]”
class-map type inspect http non_ascii_cm
   match req-resp header regex non_ascii_regex
policy-map type inspect http non_ascii_pm
   class type inspect http non_ascii_cm
      reset
```

Kop lengte inspectie — Dit commando controleert de lengte van een verzoek of antwoord header en past actie toe als de lengte de ingestelde drempel overschrijdt. Handeling is toegestaan of opnieuw ingesteld. Toevoeging van de logactie veroorzaakt een syslog bericht:

```
APPFW-4- HTTP_HEADER_LENGTH
```

Opdrachtgebruik:

```
match {request|response|req-resp} header length gt <bytes>
```

Voorbeeld van gebruikscase

Configureer een http appfw-beleid om verzoeken en antwoorden te blokkeren die een headerlengte hebben groter dan 4096 bytes.

```
class-map type inspect http hdr_len_cm
   match req-resp header length gt 4096

policy-map type inspect http hdr_len_pm
   class type inspect http hdr_len_cm
      reset
```

Kop tellen inspectie — Deze opdracht verifieert het aantal kop-lijnen (velden) in een verzoek/antwoord en past actie toe wanneer de telling de ingestelde drempel overschrijdt. Handeling is toegestaan of opnieuw ingesteld. Toevoeging van de logactie veroorzaakt een syslog bericht:

```
APPFW-6- HTTP_HEADER_COUNT
```

Opdrachtgebruik:

```
match {request|response|req-resp} header count gt <number>
```

Voorbeeld van gebruikscase

Configureer een http appfw-beleid om een verzoek te blokkeren dat meer dan 16 headervelden heeft.

```
class-map type inspect http hdr_cnt_cm
   match request header count gt 16

policy-map type inspect http hdr_cnt_pm
   class type inspect http hdr_cnt_cm
      reset
```

Kop veldinspectie — Dit commando biedt de mogelijkheid om verzoeken/antwoorden toe te staan/te weigeren/te controleren die een specifiek HTTP-headerveld en een specifieke waarde bevatten. Sta toe of stel actie terug kan worden toegepast op een verzoek of een reactie die de

klasse-kaart criteria aanpassen. De toevoeging van de logactie veroorzaakt een syslog bericht:

```
APPFW-6- HTTP_HDR_FIELD_REGEX_MATCHED
```

Opdrachtgebruik:

```
match {request|response|req-resp} header <header-name>
```

Voorbeeld van gebruikscase

Configureer een HTTP-toepassingsinspectiebeleid om spyware/adware te blokkeren:

```
parameter-map type regex ref_regex
   pattern “\.delfinproject\.com”
   pattern “\.looksmart\.com”

parameter-map type regex host_regex
   pattern “secure\.keenvalue\.com”
   pattern “\.looksmart\.com”

parameter-map type regex usragnt_regex
   pattern “Peer Points Manager”

class-map type inspect http spy_adwr_cm
   match request header refer regex ref_regex
   match request header host regex host_regex
   match request header user-agent regex usragnt_regex

policy-map type inspect http spy_adwr_pm
   class type inspect http spy_adwr_cm
      reset
```

Inspectie van veldlengte van kop — Deze opdracht biedt de mogelijkheid om de lengte van een veldlijn van kop te beperken. Sta toe of stel actie terug kan worden toegepast op een verzoek of een reactie die de klasse-kaart criteria aanpassen. De toevoeging van de logactie veroorzaakt een syslog bericht:

```
APPFW-6- HTTP_HDR_FIELD_LENGTH
```

Opdrachtgebruik:

```
match {request|response|req-resp} header <header-name> length gt <bytes>
```

Voorbeeld van gebruikscase

Configureer een http appfw-beleid om een verzoek te blokkeren waarvan de cookie- en user-agent-veldlengte respectievelijk groter is dan 256 en 128.

```
class-map type inspect http hdrline_len_cm
   match request header cookie length gt 256
   match request header user-agnet length gt 128

policy-map type inspect http hdrline_len_pm
   class type inspect http hdrline_len_cm
      reset
```

Inspectie van veldherhaling van de header — Deze opdracht controleert of een verzoek of

antwoord meerdere veldvelden heeft herhaald. Sta toe of stel actie terug kan worden toegepast op een verzoek of een reactie die de klasse-kaart criteria aanpassen. Als deze optie is ingeschakeld, veroorzaakt de logactie een syslog-bericht:

```
APPFW-6- HTTP_REPEATED_HDR_FIELDS
```

Opdrachtgebruik:

```
match {request|response|req-resp} header <header-name>
```

Voorbeeld van gebruikscase

Configureer een http appfw-beleid om een verzoek of antwoord te blokkeren dat meerdere veldheaderlijnen heeft. Dit is een van de nuttigste functionaliteiten om sessiesmokkel te voorkomen.

```
class-map type inspect http multi_occrns_cm
   match req-resp header content-length count gt 1

policy-map type inspect http multi_occrns_pm
   class type inspect http multi_occrns_cm
      reset
```

- Methode-inspectie — HTTP RFC staat een beperkte set HTTP-methoden toe. Echter, zelfs sommige standaardmethoden worden als onveilig beschouwd omdat sommige methoden kunnen worden gebruikt om kwetsbaarheden op een webserver te exploiteren. Veel van de niet-standaard methoden worden vaak gebruikt voor kwaadaardige activiteit. Dit vereist dat de methoden in verschillende categorieën worden gegroepeerd en dat de gebruiker de actie voor elke categorie kan kiezen. Deze opdracht biedt de gebruiker een flexibele manier om de methoden te groeperen in verschillende categorieën zoals veilige methoden, onveilige methoden, webdav methoden, RFC methoden en uitgebreide methoden. Sta toe of stel actie terug kan worden toegepast op een verzoek of een reactie die de klasse-kaart criteria aanpassen. Toevoeging van de logactie veroorzaakt een syslog bericht:

```
APPFW-6-HTTP_METHOD
```

Opdrachtgebruik:

```
match request method <method>
```

Voorbeeld van gebruikscase

Configureer een http appfw-beleid dat de HTTP-methoden in drie categorieën groepeert: veilig, onveilig en webdav. Deze worden in de volgende tabel getoond. Configureer handelingen zoals:

- Alle veilige methoden zijn toegestaan zonder logboekregistratie
- Alle onveilige methoden zijn toegestaan met log
- Alle webdav methoden worden geblokkeerd met log.

Veilig	onveilig	Webex DAV
KRIJG, HOOFD, OPTIE	POST, PUT, CONNECT, TRACE	BCOPY, BDELETE, BMOVE

```
http policy:
```

```
class-map type inspect http safe_methods_cm
   match request method get
   match request method head
   match request method option

class-map type inspect http unsafe_methods_cm
   match request method post
   match request method put
   match request method connect
   match request method trace

class-map type inspect http webdav_methods_cm
   match request method bcopy
   match request method bdelete
   match request method bmove

policy-map type inspect http methods_pm
   class type inspect http safe_methods_cm
      allow
   class type inspect http unsafe_methods_cm
      allow log
      class type inspect http webdav_methods_cm
      reset log
```

URI inspection— Dit commando biedt de mogelijkheid om verzoeken toe te staan/te weigeren/te monitoren waarvan de URI overeenkomt met de ingestelde reguliere inspectie. Dit geeft de gebruiker de mogelijkheid om aangepaste URL's en vragen te blokkeren. Sta toe of stel actie terug kan worden toegepast op een verzoek of een reactie die de klasse-kaart criteria aanpassen. Toevoeging van de logactie veroorzaakt een syslog bericht:

```
APPFW-6- HTTP_URI_REGEX_MATCHED
```

Opdrachtgebruik:

```
match request uri regex <parameter-map-name>
```

Voorbeeld van gebruikscase

Configureer een http appfw-beleid om een verzoek te blokkeren waarvan de URI overeenkomt met een van deze reguliere expressies:

- .*cmd.exe
- .*geslacht
- .*gokken

```
parameter-map type regex uri_regex_cm
   pattern “.*cmd.exe”
   pattern “.*sex”
   pattern “.*gambling”

class-map type inspect http uri_check_cm
   match request uri regex uri_regex_cm

policy-map type inspect http uri_check_pm
   class type inspect http uri_check_cm
      reset
```

- URI length inspection — Deze opdracht verifieert de lengte van de URI die in een verzoek

wordt verzonden en past de geconfigureerde actie toe wanneer de lengte de ingestelde drempel overschrijdt. Sta toe of stel actie terug kan worden toegepast op een verzoek of een reactie die de klasse-kaart criteria aanpassen. Toevoeging van de logactie veroorzaakt een syslog bericht:

`APPFW-6- HTTP_URI_LENGTH`

Opdrachtgebruik:

`match request uri length gt <bytes>`

Voorbeeld van gebruikscase

Configureer een http appfw-beleid om een alarm te activeren wanneer de URI-lengte van een verzoek meer dan 3076 bytes bedraagt.

```
class-map type inspect http uri_len_cm
   match request uri length gt 3076

policy-map type inspect http uri_len_pm
   class type inspect http uri_len_cm
      log
```

Argument inspection — Dit commando biedt de mogelijkheid om een verzoek waarvan de argumenten (parameters) overeenkomen met de ingestelde reguliere inspectie toe te laten, te ontkennen of te controleren. Sta toe of stel actie terug kan worden toegepast op een verzoek of een reactie die de klasse-kaart criteria aanpassen. Toevoeging van de logactie veroorzaakt een syslog bericht:

```
APPFW-6- HTTP_ARG_REGEX_MATCHED
```

Opdrachtgebruik:

```
match request arg regex <parameter-map-name>
```

Configuratie van een http appfw-beleid om een verzoek te blokkeren waarvan de argumenten overeenkomen met een van deze reguliere expressies:

- .*gecodeerd
- .*aanval

```
parameter-map type regex arg_regex_cm
   pattern “.*codered”
   pattern “.*attack”

class-map type inspect http arg_check_cm
   match request arg regex arg_regex_cm

policy-map type inspect http arg_check_pm
   class type inspect http arg_check_cm
      reset
```

- Inspectie van de lengte van het argument — Dit bevel verifieert de lengte van de argumenten die in een verzoek worden verzonden en past de gevormde actie toe wanneer de lengte gevormde drempel overschrijdt. Sta toe of stel actie terug kan worden toegepast op een verzoek of een reactie die de klasse-kaart criteria aanpassen. Toevoeging van de logactie veroorzaakt een syslog bericht:

  `APPFW-6- HTTP_ARG_LENGTH`

  Opdrachtgebruik:

  `match request arg length gt <bytes>`

Voorbeeld van gebruikscase

Configureer een http appfw-beleid om een alarm te activeren wanneer de lengte van een argument groter is dan 512 bytes.

```
class-map type inspect http arg_len_cm
   match request arg length gt 512

policy-map type inspect http arg_len_pm
   class type inspect http arg_len_cm
      log
```

- Lichaamsinspectie — Met deze CLI kan de gebruiker een lijst van reguliere expressies opgeven die moeten worden gekoppeld aan de inhoud van het verzoek of antwoord. Sta toe of stel actie terug kan worden toegepast op een verzoek of een reactie die de klasse-kaart criteria aanpassen. Toevoeging van de logactie veroorzaakt een syslog bericht: `APPFW-6- HTTP_BODY_REGEX_MATCHED`

  Opdrachtgebruik:

  `match {request|response|reg-resp} body regex <parameter-map-name>`

  Voorbeeld van gebruikscase

Configureer een http appfw om een respons te blokkeren waarvan het lichaam het patroon bevat `.*[Aa][Tt][Tt][AA][CC][Kk]`

```
parameter-map type regex body_regex
   pattern ".*[Aa][Tt][Tt][Aa][Cc][Kk]"

class-map type inspect http body_match_cm
   match response body regex body_regex

policy-map type inspect http body_match_pm
   class type inspect http body_match_cm
      reset
```

Lichaamslengteconspectie (Content) — Met deze opdracht wordt de omvang van het bericht geverifieerd dat via verzoek of antwoord wordt verstuurd. Sta toe of stel actie terug kan worden toegepast op een verzoek of een reactie die de klasse-kaart criteria aanpassen. Toevoeging van de logactie veroorzaakt een syslog bericht:

```
APPFW-4- HTTP_CONTENT_LENGTH
```

Opdrachtgebruik:

```
match {request|response|req-resp} body length lt <bytes> gt <bytes>
```

Voorbeeld van gebruikscase

Configureer een http appfw-beleid om een http-sessie te blokkeren die meer dan 10K bytes in een verzoek of antwoord bevat.

```
class-map type inspect http cont_len_cm
   match req-resp header content-length gt 10240

policy-map type inspect http cont_len_pm
   class type inspect http cont_len_cm
      reset
```

Statuslijninspectie — Met deze opdracht kan de gebruiker een lijst opgeven van reguliere

expressies die moeten worden gematcht tegen de statusregel van een respons. Sta toe of stel actie terug kan worden toegepast op een verzoek of een reactie die de klasse-kaart criteria aanpassen. Toevoeging van de logactie veroorzaakt een syslog bericht:

```
APPFW-6-HTTP_STLINE_REGEX_MATCHED
```

Opdrachtgebruik:

```
match response status-line regex <class-map-name>
```

Voorbeeld van gebruikscase

Configureer een http-app om een alarm te registreren wanneer wordt geprobeerd een verboden pagina te openen. Een verboden pagina bevat meestal een 403-statuscode en de statusregel ziet eruit als `HTTP/1.0 403-pagina verboden\r\n`.

```
parameter-map type regex status_line_regex
   pattern “[Hh][Tt][Tt][Pp][/][0-9][.][0-9][ \t]+403”

class-map type inspect http status_line_cm
   match response status-line regex status_line_regex

policy-map type inspect http status_line_pm
   class type inspect http status_line_cm
      log
```

- Content-type inspectie — Deze opdracht verifieert of het content-type van de berichtkop in de lijst met ondersteunde inhoudstypen staat. Het verifieert ook dat de inhoud-type van de kopbal de inhoud van de berichtgegevens of het gedeelte van het entiteitlichaam aanpast. Als de sleutelwoordwanverhouding wordt gevormd, verifieert het bevel het inhoudstype van het reactiebericht tegen de toegelaten gebiedswaarde van het verzoekbericht. Sta toe of stel actie terug kan worden toegepast op een verzoek of een reactie die de klasse-kaart criteria aanpassen. Toevoeging van de logactie veroorzaakt het aangewezen syslog bericht:

  ```
  APPFW-4- HTTP_CONT_TYPE_VIOLATION
  APPFW-4- HTTP_CONT_TYPE_MISMATCH
  APPFW-4- HTTP_CONT_TYPE_UNKNOWN
  ```

  Opdrachtgebruik:

  ```
  match {request|response|req-resp} header content-type [mismatch|unknown|violation]
  ```

  Voorbeeld van gebruikscaseConfigureer een http appfw-beleid om een http-sessie te blokkeren die verzoeken en antwoorden bevat die een onbekend inhoudstype hebben.

  ```
  class-map type inspect http cont_type_cm
     match req-resp header content-type unknown

  policy-map type inspect http cont_type_pm
     class type inspect http cont_type_cm
        reset
  ```

Poortmisbruikinspectie — Deze opdracht wordt gebruikt om te voorkomen dat http poort (80) wordt misbruikt voor andere toepassingen zoals IM, P2P, tunneling, enzovoort. Kan actie toestaan of resetten worden toegepast op een verzoek of antwoord dat voldoet aan de klasse-kaartcriteria. Toevoeging van de logactie veroorzaakt het aangewezen syslog bericht:

```
APPFW-4- HTTP_PORT_MISUSE_TYPE_IM
APPFW-4-HTTP_PORT_MISUSE_TYPE_P2P
APPFW-4-HTTP_PORT_MISUSE_TYPE_TUNNEL
```

Opdrachtgebruik:

```
match request port-misuse {im|p2p|tunneling|any}
```

Voorbeeld van gebruikscase

Configureer een http appfw-beleid om een http-sessie te blokkeren die voor IM-toepassing wordt misbruikt.

```
class-map type inspect http port_misuse_cm
   match request port-misuse im

policy-map type inspect http port_misuse_pm
   class type inspect http port_misuse_cm
      reset
```

- Strict-http inspection — Deze opdracht maakt strikte controle van de protocolconformiteit tegen HTTP-verzoeken en antwoorden mogelijk. Sta toe of stel actie terug kan worden toegepast op een verzoek of een reactie die de klasse-kaart criteria aanpassen. Toevoeging van de logactie veroorzaakt een syslog bericht:
  `APPFW-4- HTTP_PROTOCOL_VIOLATION`
  Opdrachtgebruik:
  `match req-resp protocol-violation`
  Voorbeeld van gebruikscaseConfigureer een http appfw-beleid om verzoeken of antwoorden te blokkeren die inbreuk maken op RFC 2616:
  ```
  class-map type inspect http proto-viol_cm
     match req-resp protocol-violation

  policy-map type inspect http proto-viol_pm
     class type inspect http proto-viol_cm
        reset
  ```
- Transfer-Encoding Inspection — Deze opdracht biedt de mogelijkheid om verzoek/antwoord toe te laten, te ontkennen of te monitoren, waarvan de overdracht encodering type overeenkomt met geconfigureerd type. Sta toe of stel actie terug kan worden toegepast op een verzoek of een reactie die de klasse-kaart criteria aanpassen. Toevoeging van de logactie veroorzaakt een syslog bericht:
  `APPFW-6- HTTP_TRANSFER_ENCODING`
  Opdrachtgebruik:
  ```
  match {request|response|req-resp} header transfer-encoding
  {regex <parameter-map-name> |gzip|deflate|chunked|identity|all}
  ```
  Voorbeeld van gebruikscaseConfigureer een http appfw-beleid om een verzoek of antwoord te blokkeren met comprimeren voor type codering.
  ```
  class-map type inspect http trans_encoding_cm
     match req-resp header transfer-encoding type compress

  policy-map type inspect http trans_encoding_pm
     class type inspect http trans_encoding_cm
        reset
  ```
- Java Applet inspection — Deze opdracht controleert of een antwoord Java-applet heeft en past de ingestelde actie toe bij detectie van applet. Sta toe of stel actie terug kan worden toegepast op een verzoek of een reactie die de klasse-kaart criteria aanpassen. Toevoeging van de logactie veroorzaakt een syslog bericht:
  `APPFW-4- HTTP_JAVA_APPLET`
  Opdrachtgebruik:
  `match response body java-applet`

Voorbeeld van gebruikscaseConfigureer een http appfw-beleid om java-applets te blokkeren.

```
class-map type inspect http java_applet_cm
   match response body java-applet

policy-map type inspect http java_applet_pm
   class type inspect http java_applet_cm
      reset
```

Ondersteuning van ZFW voor instant messaging en peer-to-peer toepassingscontrole

Cisco IOS-softwarerelease 12.4(9)T introduceerde ZFW-ondersteuning voor IM- en P2P-toepassingen.

Cisco IOS-softwarerelease 12.4(4)T biedt eerst ondersteuning voor IBM-toepassingscontrole. De eerste release van ZFW heeft IM Application in de ZFW interface niet ondersteund. Als IM applicatiecontrole gewenst was, konden gebruikers niet migreren naar de ZFW configuratie interface. Cisco IOS-softwarerelease 12.4(9)T introduceert ZFW-ondersteuning voor IM-inspectie, die Yahoo ondersteunt! Messenger (YM), MSN Messenger (MSN) en AOL Instant Messenger (AIM). Cisco IOS-softwarerelease 12.4(9)T is de eerste versie van Cisco IOS-software die native Cisco IOS-firewallondersteuning biedt voor P2P-toepassingen voor het delen van bestanden.

Zowel IM als P2P inspectie bieden Layer 4 en Layer 7 beleid voor toepassingsverkeer. Dit betekent dat ZFW fundamentele stateful inspection kan bieden om het verkeer toe te laten of te ontkennen, evenals granulaire Layer 7-controle op specifieke activiteiten in de verschillende protocollen, zodat bepaalde toepassingsactiviteiten zijn toegestaan terwijl anderen worden geweigerd.

P2P-toepassingsinspectie en -controle

SDM 2.2 introduceerde P2P-toepassingscontrole in het gedeelte Firewallconfiguratie. SDM paste een Network-Based Application Recognition (NBAR)- en QoS-beleid toe om P2P-toepassingsactiviteit te detecteren en te bewaken tot een lijnsnelheid van nul, en om al P2P-verkeer te blokkeren. Dit riep het probleem op dat CLI-gebruikers, die P2P-ondersteuning in de Cisco IOS-firewall CLI verwachtten, P2P-blokkering in de CLI niet konden configureren tenzij ze zich bewust waren van de benodigde NBAR/QoS-configuratie. Cisco IOS-softwarerelease 12.4(9)T introduceert native P2P-controle in de ZFW CLI, om NBAR te gebruiken om P2P-toepassingsactiviteit te detecteren. Deze softwarerelease ondersteunt verschillende P2P-toepassingsprotocollen:

- BitTorrent
- eDonkey
- FastTrack
- Gnutella
- KaZaA / KaZaA2
- WinMX

P2P-toepassingen zijn bijzonder moeilijk te detecteren, als gevolg van "port-hopping"-gedrag en andere trucs om detectie te vermijden, evenals problemen die worden geïntroduceerd door frequente veranderingen en updates van P2P-toepassingen die het gedrag van de protocollen wijzigen. ZFW combineert stateful inspection voor native firewalls met de traffic-recognition-functies van NBAR om P2P-toepassingscontrole te leveren in de CPL-configuratieinterface van

ZFW. NBAR biedt twee uitstekende voordelen:

- Optionele heuristische toepassingsherkenning om toepassingen te herkennen ondanks complex, moeilijk te detecteren gedrag
- Uitbreidbare infrastructuur die een updatemechanisme biedt om op de hoogte te blijven van protocolupdates en wijzigingen

P2P-inspectie configureren

Zoals eerder vermeld, biedt P2P inspectie en controle zowel Layer 4 Stateful Inspection als Layer 7 Application Control. Layer 4-inspectie is op dezelfde manier geconfigureerd als andere toepassingsservices, als de inspectie van de native Application Service-poorten toereikend is:

```
class-map type inspect match-any my-p2p-class
match protocol [bittorrent | edonkey | fasttrack | gnutella | kazaa | kazaa2 | winmx ]
[signature (optional)]
!
policy-map type inspect private-allowed-policy
 class type inspect my-p2p-class
  [drop | inspect | pass]
```

Let op de extra handtekeningsoptie in het matchprotocol [service-name]. Wanneer de handtekeningsoptie aan het eind van de verklaring van het matchprotocol wordt toegevoegd, wordt de heuristiek NBAR toegepast op het verkeer om naar tabellen in verkeer te zoeken die op specifieke P2P toepassingsactiviteit wijzen. Dit omvat port-hopping en andere veranderingen in toepassingsgedrag om verkeersopsporing te vermijden. Dit niveau van traffic inspection staat voor een verhoogd CPU-gebruik en een lagere doorvoersnelheid voor het netwerk. Als de handtekeningsoptie niet wordt toegepast, wordt de op NBAR-gebaseerde heuristische analyse niet toegepast om haven-hoppinggedrag te ontdekken, en het gebruik van cpu in niet in de zelfde mate beïnvloed.

Native service inspectie brengt het nadeel dat het niet in staat is om de controle over P2P applicaties te behouden in het geval dat de applicatie "hopt" naar een niet-standaard bron en bestemming poort, of als de applicatie wordt bijgewerkt om te beginnen actie op een niet-herkend poortnummer:

Toepassing	Native poorten (zoals herkend in 12.4(15)T PAM-lijst)
bittorrent	TCP 6881-6889
edonkey	TCP-netwerkmodule 4662
vast spoor	TCP-server 1214
gnutella	TCP 6346-6349 TCP 6355.5634 UDP 6346-6348
kazaa2	Afhankelijk van PAM
vensterbank	TCP-netwerkmodule 699

Als u P2P-verkeer wilt toestaan (inspecteren), kunt u aanvullende configuratie nodig hebben. Sommige toepassingen kunnen meerdere P2P-netwerken gebruiken of specifieke gedragingen implementeren die u in uw firewallconfiguratie moet aanpassen om de toepassing te laten werken:

- BitTorrent-clients communiceren meestal met "trackers" (peer directory servers) via http die op een niet-standaard poort draait. Dit is meestal TCP 6969, maar u kunt de torrent-specifieke tracker poort controleren. Als u BitTorrent wilt toestaan, is de beste methode om de extra poort aan te passen om HTTP te configureren als een van de overeenkomende protocollen en TCP 6969 toe te voegen aan HTTP met de opdracht ip port-map:

```
    ip port-map http port tcp 6969
```

    Je moet http en bittorrent definiëren als de matchcriteria toegepast in de class-map.
- eDonkey lijkt verbindingen te initiëren die zowel als eDonkey als Gnutella worden gedetecteerd.
- KaZaA inspectie is volledig afhankelijk van NBAR-handtekeningsdetectie.

Layer 7 (Application) Inspection verbetert Layer 4 Inspection, met de mogelijkheid om servicespecifieke acties te herkennen en toe te passen, zoals selectief blokkeren of toestaan van bestandsdoorzoeking, bestandsoverdracht en tekstchat-mogelijkheden. Service-specifieke mogelijkheden variëren per service.

P2P Application Inspection is vergelijkbaar met HTTP Application Inspection:

```
!configure the layer-7 traffic characteristics:
class-map type inspect [p2p protocol] match-any p2p-l7-cmap
 match action
!
!configure the action to be applied to the traffic
!matching the specific characteristics:
policy-map type inspect [p2p protocol] p2p-l7-pmap
 class type inspect p2p p2p-l7-cmap
  [ reset | allow ]
  log
!
!define the layer-4 inspection policy
class-map type inspect match-all p2p-l4-cmap
 match protocol [p2p protocol]
!
!associate layer-4 class and layer-7 policy-map
!in the layer-4 policy-map:
policy-map type inspect private-allowed-policy
 class type inspect p2p-l4-cmap
  [ inspect | drop | pass ]
  service-policy p2p p2p-l7-pmap
```

P2P Application Inspection biedt toepassingsspecifieke mogelijkheden voor een subset van de toepassingen die worden ondersteund door Layer 4 Inspection:

- edonkey
- vast spoor
- gnutella
- kazaa2

Elk van deze toepassingen biedt variabele applicatiespecifieke opties voor matchcriteria:

edonkey

```
router(config)#class-map type inspect edonkey match-any edonkey-l7-cmap
router(config-cmap)#match ?
  file-transfer     Match file transfer stream
  flow              Flow based QoS parameters
  search-file-name  Match file name
  text-chat         Match text-chat
```

vast spoor

```
router(config)#class-map type inspect fasttrack match-any ftrak-l7-cmap
router(config-cmap)#match ?
  file-transfer  File transfer stream
  flow           Flow based QoS parameters
```

gnutella

```
router(config)#class-map type inspect gnutella match-any gtella-l7-cmap
router(config-cmap)#
```

kazaa2

```
router(config)#class-map type inspect kazaa2 match-any kazaa2-l7-cmap
router(config-cmap)#match ?
  file-transfer  Match file transfer stream
  flow           Flow based QoS parameters
```

Nieuwe P2P protocoldefinities of updates van huidige P2P protocollen kunnen worden geladen met de dynamische pdlm update functionaliteit van NBAR. Dit is de configuratieopdracht om de nieuwe PDLM te laden:

```
ip nbar pdlm <file-location>
```

Het nieuwe protocol is beschikbaar in overeenkomende protocolopdrachten voor klassetype inspecteren. Als het nieuwe P2P protocol diensten (sub-protocollen) heeft, inspecteert de nieuwe Layer 7 klasse-map-types, evenals Layer 7-matchcriteria, worden beschikbaar.

IM-toepassingsinspectie en -controle

Cisco IOS-softwarerelease 12.4(4)T introduceerde IM-toepassingsinspectie en -controle. IM-ondersteuning is niet met ZFW geïntroduceerd in 12.4(6)T, zodat gebruikers geen IM-controle en ZFW in hetzelfde firewallbeleid konden toepassen, omdat ZFW en oudere firewallfuncties niet op een bepaalde interface kunnen samengaan.

Cisco IOS-softwarerelease 12.4(9)T ondersteunt stateful inspection en toepassingscontrole voor deze IM-services:

- AOL Instant Messenger
- MSN Messenger
- Yahoo! Messenger

De IM-inspectie verschilt enigszins van de meeste diensten, aangezien de IM-inspectie de toegang tot een specifieke groep hosts voor elke dienst controleert. De IM-diensten baseren zich over het algemeen op een relatief permanente groep directory servers, die cliënten moeten kunnen contacteren om toegang te krijgen tot de IM-dienst. IM-toepassingen zijn vaak zeer moeilijk te controleren vanuit een protocol- of servicemodel. De meest effectieve manier om deze applicaties te controleren is het beperken van de toegang tot de vaste IM servers.

IM-inspectie configureren

IM inspectie en controle biedt zowel Layer 4 Stateful inspection

en Layer 7-toepassingscontrole.

Layer 4 inspection is op dezelfde manier geconfigureerd als andere toepassingsservices:

```
class-map type inspect match-any my-im-class
match protocol [aol | msnmsgr | ymsgr ]
!
policy-map type inspect private-allowed-policy
 class type inspect my-im-class
  [drop | inspect | pass
```

IM-toepassingen kunnen op meerdere poorten contact opnemen met hun servers om hun functionaliteit te behouden. Om een bepaalde IM-dienst met de actie inspecteren toe te staan, hebt u geen serverlijst nodig om de toegestane toegang tot de servers van de IM-dienst te definiëren. Wanneer u echter een class-map configureert die een bepaalde IM-service, zoals AOL Instant Messenger, specificeert en de drop-actie toepast in de bijbehorende policy-map, kan de IM-client veroorzaken om te proberen en een andere poort te vinden waar verbinding met het internet is toegestaan. Als u geen verbinding met een bepaalde service wilt toestaan of als u de IM-servicemogelijkheden wilt beperken tot tekstchat, moet u een serverlijst definiëren zodat de ZFW verkeer kan identificeren dat aan de IM-toepassing is gekoppeld:

```
!configure the server-list parameter-map:
parameter-map type protocol-info <name>
  server name <name>
  server ip a.b.c.d
  server ip range a.b.c.d a.b.c.d
```

De Yahoo IM-serverlijst is bijvoorbeeld als volgt gedefinieerd:

```
parameter-map type protocol-info ymsgr-pmap
  server name scs.msg.yahoo.com
  server name scsd.msg.yahoo.com
  server ip 10.0.77.88
  server ip range 172.16.0.77 172.16.0.99
```

U moet de serverlijst toepassen op de protocoldefinitie:

```
class-map type inspect match-any ym-l4-cmap
 match protocol ymsgr ymsgr-pmap
```

U moet de opdrachten IP-domeinraadpleging en IP-naamserver ip.ad.re.ss configureren om naamresolutie in te schakelen.

IM-servernamen zijn vrij dynamisch. U moet periodiek controleren dat uw geconfigureerde IM server lijsten volledig en correct zijn.

Layer 7 (Application) Inspection verbetert Layer 4 Inspection, met de mogelijkheid om servicespecifieke acties te herkennen en toe te passen, zoals selectief te blokkeren of toe te staan tekstchat-mogelijkheden en ontkent andere servicemogelijkheden.

IM Application Inspection biedt momenteel de mogelijkheid om onderscheid te maken tussen tekstchat-activiteiten en alle andere applicatiediensten. Om IM-activiteit te beperken tot tekstchat, configureer een Layer 7-beleid:

```
class-map type inspect ymsgr match-any ymsgr-text-cmap
  match service text-chat
```

```
class-map type inspect ymsgr match-any ymsgr-default-cmap
  match service any

policy-map type inspect im ymsgr-l7-pmap
  class type inspect im ymsgr-text-cmap
    allow
    [log]
  class type inspect im ymsgr-text-cmap
    reset
    [log]
```

Pas het Layer 7-beleid toe op de Yahoo! Messenger beleid eerder geconfigureerd:

```
class-map type inspect match-any my-im-class
match protocol ymsgr
!
policy-map type inspect private-allowed-policy
 class type inspect my-im-class
  inspect
  service-policy im ymsgr-l7-pmap
```

URL-filters

ZFW biedt URL-filtermogelijkheden om de toegang tot webcontent te beperken tot wat is gespecificeerd door een witte of zwarte lijst die op de router is gedefinieerd, of door domeinnamen door te sturen naar een URL-filtreerserver om de toegang tot specifieke domeinen te verifiëren. ZFW URL-filtering in Cisco IOS-softwarereleases 12.4(6)T tot 12.4(15)T wordt toegepast als een extra beleidsactie die vergelijkbaar is met toepassingsinspectie.

Voor server-based URL filtering, moet u een parameter-kaart bepalen die de urlfilter serverconfiguratie beschrijft:

```
parameter-map type urlfilter websense-parmap
 server vendor [n2h2 | websense] 10.1.1.1
```

Als statische witte of zwarte lijsten de voorkeur hebben, kunt u een lijst van domeinen of subdomeinen bepalen die specifiek worden toegestaan of ontkend, terwijl de omgekeerde actie wordt toegepast op verkeer dat niet de lijst aanpast:

```
parameter-map type urlfilter websense-parmap
 exclusive-domain deny .disallowed.com
 exclusive-domain permit .cisco.com
```

Als een zwarte lijst URL is gedefinieerd met ontkennen opties in de exclusieve domeindefinities, zijn alle andere domeinen toegestaan. Als er "vergunningen" zijn gedefinieerd, moeten alle toegestane domeinen expliciet worden gespecificeerd, vergelijkbaar met de functie van IP-toegangscontrolelijsten.

Stel een class-map in die overeenkomt met HTTP-verkeer:

```
class-map type inspect match-any http-cmap
 match protocol http
```

Definieer een policy-map die uw class-map koppelt aan inspect en urlfilter acties:

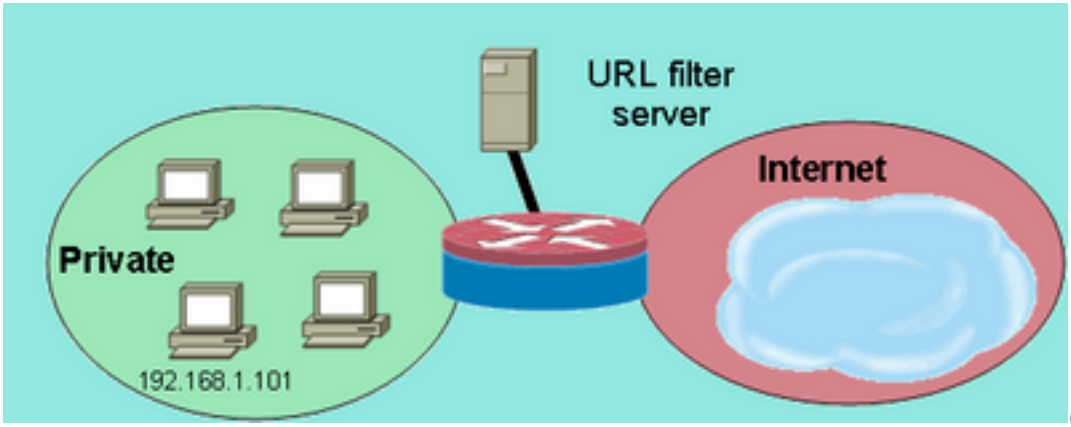
```
policy-map type inspect http-filter-pmap
```

```
 class type inspect http-cmap
  inspect
  urlfilter websense-parmap
```

Dit vormt de minimumvereiste om met een URL-filtreerserver te communiceren. Er zijn verschillende opties beschikbaar om aanvullend URL-filtergedrag te definiëren.

Sommige netwerkimplementaties willen URL-filtering toepassen voor sommige hosts of subnetten en URL-filtering voor andere hosts omzeilen. Bijvoorbeeld, in afbeelding 9, moeten alle hosts in de privé-zone HTTP-verkeer gecontroleerd door een URL-filterserver, behalve de specifieke host 192.168.1.101.

Afbeelding 10: URL-filtering van voorbeeldtopologie



URL-filtering van voorbeeldtopologie

Dit kan worden bereikt als u twee verschillende klasse-kaart kaarten definieert:

- Eén class-map die alleen HTTP-verkeer aanpast voor de grotere groep hosts die URL-filtering ontvangen.
- Eén class-map voor de kleinere groep hosts, die geen URL-filtering ontvangen. De tweede klasse-kaart komt overeen met HTTP-verkeer en een lijst met hosts die zijn vrijgesteld van het URL-filterbeleid.

Beide class-maps worden geconfigureerd in een policy-map, maar slechts één ontvangt de urlfilter actie:

```
class-map type inspect match-any http-cmap
 match protocol http
class-map type inspect match-all http-no-urlf-cmap
 match protocol http
 match access-group 101
!
policy-map type inspect http-filter-pmap
 class type inspect http-no-urlf-cmap
  inspect
 class type inspect http-cmap
  inspect
  urlfilter websense-parmap
!
access-list 101 permit ip 192.168.1.101 any
```

Control Access naar de router

De meeste ingenieurs van de netwerkveiligheid zijn oncomfortabel als zij de het beheersinterfaces van de router (bijvoorbeeld, SSH, Telnet, HTTP, HTTPS, SNMP, etc.) aan openbaar Internet

blootstellen, en onder bepaalde omstandigheden, is de controle nodig voor LAN toegang tot de router eveneens. Cisco IOS-software biedt een aantal opties om toegang tot de verschillende interfaces te beperken, waaronder de functiefamilie Network Foundation Protection (NFP), verschillende toegangscontrolemechanismen voor beheerinterfaces en de zelfzone van ZFW. U moet andere functies, zoals VTY-toegangscontrole, bescherming van het beheervliegtuig en SNMP-toegangscontrole bekijken om te bepalen welke combinatie van routerbeheerfuncties het beste werkt voor uw specifieke toepassing.

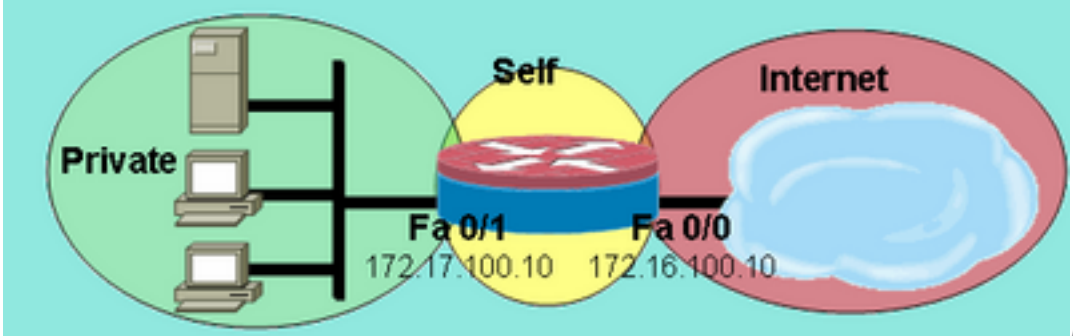
Over het algemeen, is de NFP eigenschapfamilie meest geschikt voor controle van verkeer dat voor de router zelf wordt bestemd. Raadpleeg Control Plane Security Overzicht in Cisco IOS-software voor informatie over routerbescherming met de NFP-functies.

Als u besluit om ZFW toe te passen om verkeer te besturen van en naar de IP-adressen op de router zelf, moet u begrijpen dat het standaard firewallbeleid en de functies verschillen van die beschikbaar voor transitverkeer. Transit verkeer wordt gedefinieerd als netwerkverkeer waarvan de bron- en bestemmings-IP-adressen niet overeenkomen met IP-adressen die op een van de routerinterfaces worden toegepast, en het verkeer veroorzaakt niet dat de router bijvoorbeeld netwerkcontroleberichten zoals verloopdatums van ICMP TTL of onbereikbare berichten voor netwerk/host verstuurt.

ZFW past een standaard deny-all beleid toe op verkeer dat zich tussen zones beweegt, behalve, zoals vermeld in de algemene regels, verkeer in elke zone die direct naar de adressen van de interfaces van de router vloeit impliciet is toegestaan. Dit verzekert dat de connectiviteit aan de beheersinterfaces van de router wordt gehandhaafd wanneer een configuratie van de streekfirewall op de router wordt toegepast. Als de zelfde ontkennen-alle beleid beïnvloedde connectiviteit rechtstreeks aan de router, zou een volledige configuratie van het beheersbeleid moeten worden toegepast alvorens de streken op de router worden gevormd. Dit zou waarschijnlijk de beheersconnectiviteit verstoren als het beleid verkeerd werd uitgevoerd of in de verkeerde volgorde werd toegepast.

Wanneer een interface wordt geconfigureerd om een zone lid te zijn, zijn de hosts die zijn aangesloten op de interface inbegrepen in de zone. Verkeer dat naar en van de IP-adressen van de interfaces van de router stroomt, wordt echter niet bepaald door het zonebeleid (met uitzondering van de omstandigheden die in de opmerking in afbeelding 10 worden beschreven). In plaats daarvan, worden alle IP interfaces op de router automatisch gemaakt deel van de zelf-streek wanneer ZFW wordt gevormd. Om IP-verkeer te controleren dat zich naar de interfaces van de router verplaatst vanuit de verschillende zones op een router, moet beleid worden toegepast om verkeer tussen de zone en de zelfzone van de router te blokkeren of toe te staan/te inspecteren, en omgekeerd (zie afbeelding 11).

Afbeelding 11: Beleid toepassen tussen netwerkzones en routerzelfzone



Beleid toepassen tussen netwerkzones en routerzelfzone

Hoewel de router een standaard-sta beleid tussen alle zones en de zelf-zone aanbiedt, als een beleid van om het even welke zone aan de zelf-zone wordt gevormd, en geen beleid van zelf aan de gebruiker-configureerbare interface-connected zones van de router wordt gevormd, ontmoet al router-voortgekomen verkeer de verbonden-zone aan zelf-streek beleid bij zijn terugkeer van de router en geblokkeerd. Aldus, moet het router-voortgekomen verkeer worden geïnspecteerd om zijn terugkeer naar de zelf-streek toe te staan.

> **Opmerking:** Cisco IOS-software gebruikt altijd het IP-adres dat aan een interface- "dichtstbijzijnde" bestemmingshost is gekoppeld voor verkeer, zoals syslog, tftp, telnet en andere besturingsplane-services, en onderwerpt dit verkeer aan een firewallbeleid in een zelfzone. Als een service echter een specifieke interface definieert als de bron-interface met opdrachten die bestaan uit, maar niet beperkt zijn tot, het vastleggen van de bron-interface [type nummer], de ip tftp bron-interface [type nummer] en de ip telnet bron-interface [type nummer] , wordt het verkeer onderworpen aan de zelfzone.

> **Opmerking**:Sommige services (met name de spraak-over-IP-services van routers) maken gebruik van tijdelijke of niet-configureerbare interfaces die niet aan beveiligingszones kunnen worden toegewezen. Deze services kunnen niet goed functioneren als hun verkeer niet kan worden gekoppeld aan een geconfigureerde beveiligingszone.

Beleidsbeperkingen voor zelfzone

Zelfzonebeleid heeft een beperkte functionaliteit in vergelijking met het beleid dat beschikbaar is voor transitoverkeerszoneparen:

- Zoals het geval was met klassieke stateful inspection, is het routerverkeer beperkt tot TCP, UDP, ICMP en complexe protocolinspectie voor H.323.
- Application Inspection is niet beschikbaar voor beleid in zelfzones.
- Sessiebeperkingen en snelheidsbeperkingen kunnen niet worden geconfigureerd op basis van zelfzonebeleid.

Beleidsconfiguratie voor zelfzone

Onder de meeste omstandigheden, zijn dit wenselijk toegangsbeleid voor de diensten van het routerbeheer:

- Ontken alle connectiviteit van Telnet, aangezien het duidelijke tekstprotocol van Telnet gebruikersreferenties en andere gevoelige informatie gemakkelijk blootstelt.
- Sta SSH-verbindingen toe van elke gebruiker in elke zone. SSH versleutelt gebruikersreferenties en sessiegegevens, die bescherming bieden tegen kwaadaardige gebruikers die pakketopnametools gebruiken om te kijken naar gebruikersactiviteit en gebruikersreferenties of gevoelige informatie zoals routerconfiguratie te compromitteren. SSH versie 2 biedt sterkere bescherming en pakt specifieke kwetsbaarheden aan die inherent zijn aan SSH versie 1.
- Sta HTTP connectiviteit aan de router van de privé zones toe als de privé zone betrouwbaar is. Anders, als de privé zone het potentieel voor kwaadwillige gebruikers om informatie te compromitteren herbergt, gebruikt HTTP geen encryptie om beheersverkeer te beschermen, en kan gevoelige informatie zoals gebruikersgeloofsbrieven of configuratie openbaren.

- HTTPS-connectiviteit vanuit elke zone toestaan. Overeenkomstig met SSH versleutelt HTTPS sessiegegevens en gebruikersreferenties.
- Beperk SNMP-toegang tot een specifieke host of subnetverbinding. SNMP kan worden gebruikt om routerconfiguratie aan te passen en configuratieinformatie te onthullen. SNMP moet worden geconfigureerd met toegangscontrole voor de verschillende gemeenschappen.
- Blokkeer ICMP-verzoeken van het openbare internet naar het privaat-zoneadres (hierbij wordt aangenomen dat het privaat-zoneadres routable is). Eén of meer openbare adressen kunnen indien nodig worden blootgesteld aan ICMP-verkeer voor probleemoplossing in het netwerk. Verschillende ICMP-aanvallen kunnen worden gebruikt om routerbronnen te overweldigen of netwerktopologie en architectuur te herkennen.

Een router kan dit type van beleid met de toevoeging van twee streek-paren voor elke streek toepassen die moet worden gecontroleerd. Elk zone-paar voor verkeer naar of vanuit de router zelf-zone moet worden aangepast door het respectievelijke beleid in de tegenovergestelde richting, tenzij verkeer niet in de tegenovergestelde richting wordt gegenereerd. Er kan één policy-map voor zowel inkomende als uitgaande zone-paren worden toegepast die al het verkeer beschrijft, of er kunnen specifieke policy-maps per zone-paar worden toegepast. De configuratie van specifieke zone-paren per beleid-kaart verstrekt granularity om activiteit te bekijken die elke beleid-kaart aanpast.

Een voorbeeldnetwerk met een SNMP-beheerstation op 172.17.100.11 en een TFTP-server op 172.17.100.17, deze uitvoer biedt een voorbeeld van het gehele toegangsbeleid voor de beheer-interface:

```
class-map type inspect match-any self—service-cmap
 match protocol tcp
 match protocol udp
 match protocol icmp
 match protocol h323
!
class-map type inspect match-all to-self-cmap
 match class-map self—service-cmap
 match access-group 120
!
class-map type inspect match-all from-self-cmap
 match class-map self—service-cmap
!
class-map type inspect match-all tftp-in-cmap
 match access-group 121
!
class-map type inspect match-all tftp-out-cmap
 match access-group 122
!
policy-map type inspect to-self-pmap
 class type inspect to-self-cmap
  inspect
 class type inspect tftp-in-cmap
  pass
!
policy-map type inspect from-self-pmap
 class type inspect from-self-cmap
  inspect
 class type inspect tftp-out-cmap
  pass
!
zone security private
zone security internet
```

```
zone-pair security priv-self source private destination self
 service-policy type inspect to-self-pmap
zone-pair security net-self source internet destination self
 service-policy type inspect to-self-pmap
zone-pair security self-priv source self destination private
 service-policy type inspect from-self-pmap
zone-pair security self-net source self destination internet
 service-policy type inspect from-self-pmap

!
interface FastEthernet 0/0
 ip address 172.16.100.10
 zone-member security internet
!
interface FastEthernet 0/1
 ip address 172.17.100.10
 zone-member security private
!
access-list 120 permit icmp 172.17.100.0 0.0.0.255 any
access-list 120 permit icmp any host 172.17.100.10 echo
access-list 120 deny icmp any any
access-list 120 permit tcp 172.17.100.0 0.0.0.255 host 172.17.100.10 eq www
access-list 120 permit tcp any any eq 443
access-list 120 permit tcp any any eq 22
access-list 120 permit udp any host 172.17.100.10 eq snmp
access-list 121 permit udp host 172.17.100.17 host 172.17.100.10
access-list 122 permit udp host 172.17.100.10 host 172.17.100.17
```

Helaas biedt het zelfzonebeleid niet de mogelijkheid om TFTP-overdrachten te inspecteren. Aldus, moet de firewall al verkeer aan en van de server van TFTP overgaan als TFTP door de firewall moet overgaan.

Als de router IPsec VPN-verbindingen beëindigt, moet u ook een beleid definiëren om IPSec ESP, IPSec AH, ISAKMP en NAT-T IPSec (UDP 4500) over te gaan. Dit is afhankelijk van welke diensten u nodig heeft. Dit volgende beleid kan worden toegepast naast het hierboven genoemde beleid. Merk de verandering in de beleid-kaarten waar een klasse-kaart voor het verkeer van VPN met een pasactie is opgenomen op. Typisch, is het gecodeerde verkeer betrouwbaar, tenzij uw veiligheidsbeleid verklaart dat u gecodeerd verkeer aan en van gespecificeerde endpoints moet toestaan.

```
class-map type inspect match-all crypto-cmap
 match access-group 123
!
policy-map type inspect to-self-pmap
 class type inspect crypto-cmap
  pass
 class type inspect to-self-cmap
  inspect
 class type inspect tftp-in-cmap
  pass
!
policy-map type inspect from-self-pmap
 class type inspect crypto-cmap
  pass
 class type inspect from-self-cmap
  inspect
 class type inspect tftp-out-cmap
  pass
!
access-list 123 permit esp any any
access-list 123 permit udp any any eq 4500
```

```
access-list 123 permit ah any any
access-list 123 permit udp any any eq 500
```

Zone-gebaseerde firewall en Wide Area Application Services

Raadpleeg Releaseopmerking voor Cisco Wide Area Application Services (Software versie 4.0.13) - Nieuwe functies voor Software versie 4.0.13 voor een toepassingsopmerking die configuratievoorbeelden en gebruikshandleidingen biedt

Monitor Zone-Based Policy Firewall met opdrachten tonen en debuggen

ZFW introduceert nieuwe opdrachten om de beleidsconfiguratie te bekijken en de firewallactiviteit te bewaken.

Beschrijving van weergavezone en de interfaces in een bepaalde zone:

```
show zone security [<zone-name>]
```

Wanneer de zonenaam niet inbegrepen is, toont het bevel de informatie van alle gevormde streken.

```
Router#show zone security z1
zone z1
  Description: this is test zone1
  Member Interfaces:
    Ethernet0/0
```

Toont de bronzone, de bestemmingszone en het beleid in bijlage aan het zone-paar:

```
show zone-pair security [source <source-zone-name>] [destination <destination-zone-name>]
```

Wanneer geen bron of bestemming wordt gespecificeerd, worden alle zone-paren met bron, bestemming, en het bijbehorende beleid getoond. Wanneer alleen de bron/bestemming zone wordt vermeld, worden alle zone-paren die deze zone bevatten als de bron/bestemming weergegeven.

```
Router#show zone-pair security
zone-pair name zp
  Source-Zone z1  Destination-Zone z2
  service-policy p1
```

Toont een gespecificeerde beleidskaart:

```
show policy-map type inspect [<policy-map-name> [class <class-map-name]]
```

Wanneer de naam van een policy-map niet is gespecificeerd, worden alle policy-maps van het type geïnspecteerd (samen met Layer 7 policy-maps die een subtype bevatten).

```
Router#show policy-map type inspect p1
 Policy Map type inspect p1
   Class c1
    Inspect
```

Toont de runtime inspecteren type beleid-kaart statistieken momenteel op een gespecificeerde streek-paar.

```
show policy-map type inspect zone-pair [zone-pair-name] [sessions]
```

Wanneer geen zone-paar naam wordt vermeld, worden beleidskaarten op alle zone-paren weergegeven.

De sessiesoptie geeft de inspectiesessies weer die door de policy-map-toepassing op de opgegeven zone-paar zijn gemaakt.

```
Router#show policy-map type inspect zone-pair zp
 Zone-pair: zp

  Service-policy : p1

    Class-map: c1 (match-all)
      Match: protocol tcp
      Inspect
        Session creations since subsystem startup or last reset 0
        Current session counts (estab/half-open/terminating) [0:0:0]
        Maxever session counts (estab/half-open/terminating) [0:0:0]
        Last session created never
        Last statistic reset never
        Last session creation rate 0
        Last half-open session total 0

    Class-map: c2 (match-all)
      Match: protocol udp
      Pass
        0 packets, 0 bytes

    Class-map: class-default (match-any)
      Match: any
      Drop
        0 packets, 0 bytes
```

Het sleutelwoord urlfilter toont de urlfilter-gerelateerde statistieken die betrekking hebben op de gespecificeerde beleid-kaart (of beleid-kaarten op alle doelstellingen wanneer geen zone-paar naam wordt gespecificeerd):

```
show policy-map type inspect zone-pair [zone-pair-name] [urlfilter [cache]]
```

Wanneer het cachesleutelwoord samen met urlfilter wordt gespecificeerd, toont het het urlfiltercachegeheugen (van IP-adressen).

Samenvatting van de opdracht beleidskaart voor show voor inspecteren van beleidskaarten:

```
show policy-map type inspect inspect { <policy name> [class <class name>] |
                  zone-pair [<zone-pair name>] [sessions | urlfilter cache] }
```

Tune Zone-Based Policy Firewall - Bescherming tegen weigering van service

ZFW biedt DoS-bescherming om netwerkengineers te waarschuwen voor dramatische veranderingen in netwerkactiviteit en om ongewenste activiteit te beperken om de impact van veranderingen in netwerkactiviteit te verminderen. ZFW houdt een aparte teller aan voor de klassenkaart van elke beleidskaart. Dus, als één klasse-kaart wordt gebruikt voor twee verschillende zone-paren' beleid-kaarten, worden twee verschillende reeksen van DoS-beschermingstellers toegepast.

ZFW biedt standaard DoS-aanvalsbeperking op Cisco IOS-softwarereleases vóór 12.4(11)T. Het standaard DoS-beschermingsgedrag is gewijzigd met Cisco IOS-softwarerelease 12.4(11)T.

Raadpleeg Defining Strategies to Protect Against TCP SYN Denial of Service Attacks voor meer informatie over TCP SYN DoS-aanvallen.

Aanhangsels

Bijlage A: Basisconfiguratie

```
ip subnet-zero
ip cef
!
bridge irb
!
interface FastEthernet0
 ip address 172.16.1.88 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet1
 ip address 172.16.2.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet2
 switchport access vlan 2
!
interface FastEthernet3
 switchport access vlan 2
!
interface FastEthernet4
 switchport access vlan 1
!
interface FastEthernet5
 switchport access vlan 1
!
interface FastEthernet6
 switchport access vlan 1
!
interface FastEthernet7
 switchport access vlan 1
!
interface Vlan1
 no ip address
```

```
 bridge-group 1
!
interface Vlan2
 no ip address
 bridge-group 1
!
interface BVI1
 ip address 192.168.1.254 255.255.255.0
 ip route-cache flow
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.16.1.1
!
bridge 1 protocol ieee
bridge 1 route ip
!
end
```

Bijlage B: Laatste (volledige) configuratie

```
ip subnet-zero
ip cef
!
ip port-map user-Xwindows port tcp from 6900 to 6910
!
class-map type inspect match-any L4-inspect-class
 match protocol tcp
 match protocol udp
 match protocol icmp
class-map type inspect match-any L7-inspect-class
  match protocol ssh
  match protocol ftp
  match protocol pop
  match protocol imap
  match protocol esmtp
  match protocol http
class-map type inspect match-any dns-http-class
 match protocol dns
 match protocol http
class-map type inspect match-any smtp-class
 match protocol smtp
class-map type inspect match-all dns-http-acl-class
 match access-group 110
 match class-map dns-http-class
class-map type inspect match-all smtp-acl-class
 match access-group 111
 match class-map smtp-class
class-map type inspect match-any Xwindows-class
 match protocol user-Xwindows
class-map type inspect match-any internet-traffic-class
 match protocol http
 match protocol https
 match protocol dns
 match protocol icmp
class-map type inspect http match-any bad-http-class
 match  port-misuse all
 match  strict-http
!
policy-map type inspect clients-servers-policy
 class type inspect L4-inspect-class
  inspect
policy-map type inspect private-dmz-policy
  class type inspect L7-inspect-class
```

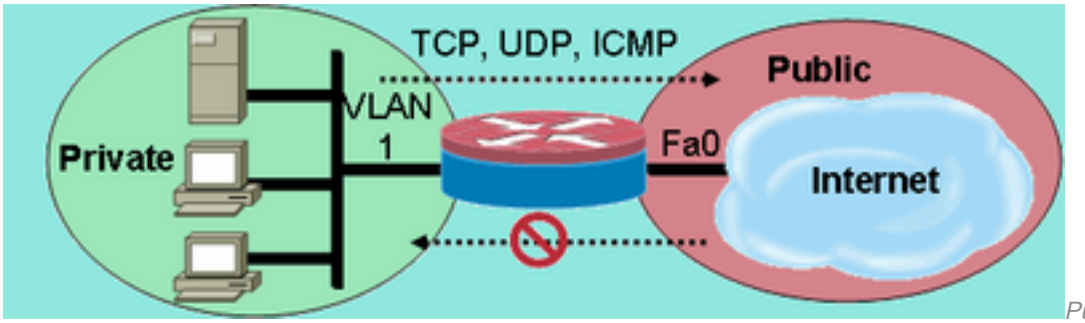
```
   inspect
policy-map type inspect internet-dmz-policy
 class type inspect dns-http-acl-class
  inspect
 class type inspect smtp-acl-class
  inspect
policy-map type inspect servers-clients-policy
 class type inspect Xwindows-class
  inspect
policy-map type inspect private-internet-policy
  class type inspect internet-traffic-class
   inspect
  class type inspect bad-http-class
   drop
!
zone security clients
zone security servers
zone security private
zone security internet
zone security dmz
zone-pair security private-internet source private destination internet
  service-policy type inspect private-internet-policy
zone-pair security servers-clients source servers destination clients
  service-policy type inspect servers-clients-policy
zone-pair security clients-servers source clients destination servers
  service-policy type inspect clients-servers-policy
zone-pair security private-dmz source private destination dmz
  service-policy type inspect private-dmz-policy
zone-pair security internet-dmz source internet destination dmz
  service-policy type inspect internet-dmz-policy
!
bridge irb
!
interface FastEthernet0
 ip address 172.16.1.88 255.255.255.0
 zone-member internet
!
interface FastEthernet1
 ip address 172.16.2.1 255.255.255.0
 zone-member dmz
!
interface FastEthernet2
 switchport access vlan 2
!
interface FastEthernet3
 switchport access vlan 2
!
interface FastEthernet4
 switchport access vlan 1
!
interface FastEthernet5
 switchport access vlan 1
!
interface FastEthernet6
 switchport access vlan 1
!
interface FastEthernet7
 switchport access vlan 1
!
interface Vlan1
 no ip address
 zone-member clients
 bridge-group 1
!
```

```
interface Vlan2
 no ip address
 zone-member servers
 bridge-group 1
!
interface BVI1
 ip address 192.168.1.254 255.255.255.0
 zone-member private
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.16.1.1
!
access-list 110 permit ip any host 172.16.2.2
access-list 111 permit ip any host 172.16.2.3
!
bridge 1 protocol ieee
bridge 1 route ip
!
End
```

Bijlage C: Configuratie van firewall voor basiszone-beleid voor twee zones

Dit voorbeeld biedt een eenvoudige configuratie als basis om functies te testen voor verbeteringen van de Cisco IOS-software ZFW. Deze configuratie is een modelconfiguratie voor twee zones, zoals geconfigureerd op een 1811-router. De privé-zone wordt toegepast op de vaste routerpoorten van de switch, zodat alle hosts op de switch-poorten zijn verbonden met VLAN 1. De openbare zone wordt toegepast op Fast Ethernet 0 (zie afbeelding 12).

Afbeelding 12: Public Zone toegepast op Fast Ethernet 0



Public Zone toegepast op Fast Ethernet 0

```
class-map type inspect match-any private-allowed-class
 match protocol tcp
 match protocol udp
 match protocol icmp
class-map type inspect match-all http-class
 match protocol http
!
policy-map type inspect private-allowed-policy
 class type inspect http-class
  inspect my-parameters
 class type inspect private-allowed-class
  inspect
!
zone security private
zone security public
zone-pair security priv-pub source private destination public
 service-policy type inspect private-allowed-policy
!
interface fastethernet 0
```

```
 zone-member security public
!
interface VLAN 1
 zone-member security private
```

Gerelateerde informatie

- Technische ondersteuning en documentatie – Cisco Systems

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.