Entender o design do firewall de política baseado em zona

Contents

Introduction

Este documento descreve o modelo de configuração do conjunto de recursos do Cisco IOS® Firewall, Zone-based Policy Firewall (ZFW).

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Informações de Apoio

Esse novo modelo de configuração oferece políticas intuitivas para roteadores de várias interfaces, maior granularidade de aplicação de política de firewall e uma política padrão de negação total que proíbe tráfego entre zonas de segurança de firewall até uma política explícita aplicada para permitir o tráfego desejável.

Quase todos os recursos clássicos do Cisco IOS Firewall implementados antes da versão de software do Cisco IOS 12.4(6)T são aceitos na nova interface de inspeção de política de acordo com a zona:

- Inspeção de pacotes stateful
- Cisco IOS Firewall compatível com VRF
- Filtragem de URL
- Mitigação de negação de serviço (DoS)

O software Cisco IOS versão 12.4(9)T adicionou o suporte ZFW para os limites de taxa de transferência e sessão/conexão por classe, além de controle e inspeção de aplicação:

- HTTP
- Post Office Protocol (POP3), Internet Mail Access Protocol (IMAP), Simple Mail Transfer Protocol/Enhanced Simple Mail Transfer Protocol (SMTP/ESMTP)
- RPC (chamada de procedimento remoto) da Sun
- Aplicações de mensagens instantâneas (IM):Microsoft MessengerYahoo! Messenger(por exemplo: Instant Messenger)
- Compartilhamento de arquivos peer-to-peer (P2P):BitTorrentKaZaAGnutellaeDonkey

O software Cisco IOS versão 12.4(11)T adicionou estatísticas para facilitar o ajuste de proteção DoS.

Alguns recursos e funcionalidades do firewall clássico do Cisco IOS ainda não são compatíveis em um ZFW no software Cisco IOS versão 12.4(15)T:

- Proxy de autenticação
- Failover de firewall stateful
- MIB de firewall unificado
- Inspeção stateful IPv6
- Suporte de TCP fora de serviço

O ZFW geralmente melhora o desempenho do Cisco IOS para a maioria das atividades de inspeção do firewall. Nem o Cisco IOS ZFW nem o Classic Firewall incluem suporte à inspeção stateful para tráfego multicast.

Resumo da política de acordo com a zona

A inspeção stateful do Cisco IOS Classic Firewall (anteriormente conhecida como controle de acesso baseado em contexto ou CBAC) empregava um modelo de configuração de acordo com a interface, no qual uma política de inspeção stateful era aplicada a uma interface. Todo o tráfego que passa por essa interface recebeu a mesma política de inspeção. Esse modelo de configuração limitou a granularidade das políticas de firewall e ocasionou uma confusão sobre a aplicação adequada de políticas de firewall, especialmente em cenários quando as políticas de firewall devem ser aplicadas entre várias interfaces.

O firewall de política de acordo com a zona (também conhecido como firewall de política de zona ou ZFW) altera a configuração de firewall do modelo antigo de acordo com a interface para um modelo baseado em zona mais flexível e fácil de entender. As interfaces são atribuídas a zonas e a política de inspeção é aplicada ao tráfego que se move entre as zonas. As políticas entre as zonas oferecem flexibilidade e granularidade consideráveis; portanto, políticas de inspeção diferentes podem ser aplicadas a vários grupos de hosts conectados à mesma interface do roteador.

As políticas de firewall são configuradas com o Cisco Policy Language (CPL), que emprega uma estrutura hierárquica para definir a inspeção de protocolos de rede e os grupos de hosts aos quais a inspeção pode ser aplicada.

Modelo de configuração de política de acordo com a zona

O ZFW altera completamente a maneira pela qual você configura uma inspeção do Cisco IOS Firewall, em comparação com o firewall clássico do Cisco IOS.

A primeira grande alteração na configuração do firewall é a introdução da configuração de acordo com a zona. O Cisco IOS Firewall é o primeiro recurso de defesa contra ameaças do software Cisco IOS para implementar um modelo de configuração de zona. Outros recursos podem adotar o modelo de zona ao longo do tempo. O modelo de configuração de acordo com a interface da inspeção stateful do Cisco IOS Classic Firewall (ou CBAC) que emprega o conjunto de comandos ip inspect é mantido por um período. No entanto, poucos novos recursos, se houver, são configuráveis com a interface de linha de comando clássica (CLI). O ZFW não usa os comandos de inspeção stateful ou CBAC. Os dois modelos de configuração podem ser usados simultaneamente nos roteadores, porém não combinados em interfaces. Uma interface não pode ser configurada como um membro de zona de segurança e, ao mesmo tempo, configurada para ip inspect .

As zonas estabelecem as bordas de segurança da rede. Uma zona define um limite onde o tráfego está sujeito a restrições de política, pois atravessa para outra região da rede. A política padrão ZFW entre regiões é deny all. Se nenhuma política estiver configurada explicitamente, todo o tráfego que se move entre as zonas será bloqueado. Essa é uma partida significativa do modelo de inspeção stateful, em que o tráfego era implicitamente permitido até ser explicitamente bloqueado com uma lista de controle de acesso (ACL).

A segunda grande alteração é a introdução de uma nova linguagem de política de configuração conhecida como CPL. Os usuários familiarizados com a CLI de Qualidade de Serviço (QoS - Modular Quality-of-Service) do Software Cisco IOS (MQC - Modular Quality-of-Service) podem reconhecer que o formato é semelhante ao uso de mapas de classe para especificar qual tráfego é afetado pela ação aplicada em um mapa de política.

Regras Para Aplicativo De Firewall De Diretiva Baseada Em Zona

As associações de interface de rede do roteador em zonas estão sujeitas a várias regras que controlam o comportamento da interface, assim como o tráfego que se move entre as interfaces de membro de zona:

- Uma zona deve ser configurada antes da atribuição das interfaces.
- Uma interface pode ser atribuída a apenas uma zona de segurança.
- Todo o tráfego de entrada e saída da interface é implicitamente bloqueado, quando a interface é atribuída a uma zona, exceto o tráfego de entrada e saída de outras interfaces na mesma zona e o tráfego de entrada em qualquer interface no roteador.
- O tráfego é implicitamente autorizado a fluir por padrão entre as interfaces que são membros da mesma zona.
- Para permitir o tráfego de e para uma interface de membro de zona, uma política que permite

ou inspeciona o tráfego deve ser configurada entre essa zona e qualquer outra zona.
- A zona própria é a única exceção à política padrão deny all. Todo o tráfego para qualquer interface de roteador é permitido até que ele seja negado explicitamente.
- O tráfego não pode fluir entre uma interface membro da zona e qualquer interface que não seja um membro da zona. As ações de aprovação, inspeção e descarte só podem ser aplicadas entre duas zonas.
- As interfaces que não foram atribuídas a uma função de região como portas de roteador clássicas e ainda podem usar a inspeção stateful clássica/configuração CBAC.
- Se for necessário que uma interface na caixa não faça parte da política de zona/firewall. Ainda pode ser necessário colocar essa interface em uma região e configurar uma política Passar tudo (tipo de política fictícia) entre essa região e qualquer outra região para a qual o fluxo de tráfego é desejado.
- A partir do comportamento anterior, segue-se que, se o tráfego for fluir entre todas as interfaces em um roteador, todas as interfaces devem ser parte do modelo de zoneamento (cada interface deve ser um membro de uma zona ou outra).
- A única exceção ao comportamento anterior, deny por padrão, é o tráfego de e para o roteador, que é permitido por padrão. Uma política explícita pode ser configurada para restringir esse tráfego.

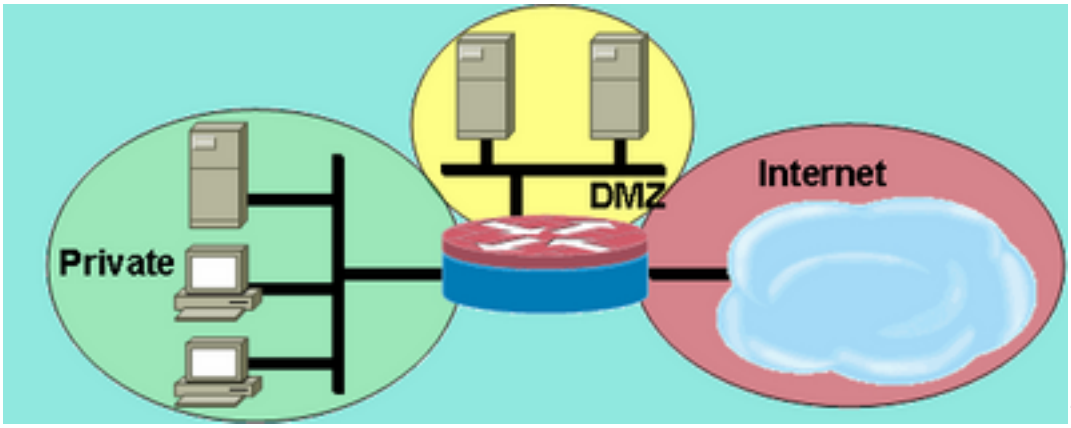
Projetar Segurança de Rede com Política Baseada em Zona

Uma zona de segurança deve ser configurada para cada região de segurança relativa dentro da rede, para que todas as interfaces atribuídas à mesma zona sejam protegidas com um nível de segurança semelhante. Por exemplo, considere um roteador de acesso com três interfaces:

- Uma interface conectada à Internet pública
- Uma interface conectada a uma LAN privada não deve ser acessada da Internet pública
- Uma interface conectada a uma zona desmilitarizada (DMZ) do serviço de Internet, em que um servidor Web, servidor DNS (Sistema de nomes de domínio) e servidor de e-mail devem estar acessíveis à Internet pública

Cada interface nessa rede é atribuída a sua própria zona, embora você possa permitir acesso variado da Internet pública a hosts específicos na DMZ e políticas de uso de aplicativos variadas para hosts na LAN protegida. (Consulte a Figura 1.)

Figura 1: Topologia básica de zona de segurança



Topologia básica de zona de segurança

Neste exemplo, cada zona contém apenas uma interface. Se uma interface adicional for

adicionada à região privada, os hosts conectados à nova interface na região poderão passar o tráfego para todos os hosts na interface atual na mesma região. Além disso, o tráfego de host para hosts em outras zonas é igualmente afetado pelas políticas atuais.

Geralmente, a rede do exemplo tem três políticas principais:

- Conectividade de zona privada à Internet
- Conectividade de zona privada a hosts DMZ
- Conectividade de zona de Internet a hosts DMZ

Como a DMZ é exposta à Internet pública, os hosts da DMZ podem estar sujeitos a atividades indesejadas de indivíduos mal-intencionados que podem danificar um ou mais hosts da DMZ. Se nenhuma política de acesso for fornecida para que os hosts DMZ acessem os hosts da zona privada ou da zona da Internet, os indivíduos que comprometeram os hosts DMZ não poderão usar os hosts DMZ para realizar ataques adicionais contra hosts privados ou da Internet. O ZFW impõe uma postura de segurança padrão proibitiva. Portanto, a menos que os hosts DMZ tenham especificamente acesso a outras redes, elas são protegidas contra qualquer conexão dos hosts DMZ. Da mesma forma, nenhum acesso é fornecido para os hosts da Internet acessarem os hosts de zona privados; portanto, os hosts de zona privados estão protegidos contra o acesso indesejado dos hosts da Internet.

Usar VPN IPSec com firewall de política baseado em zona

Melhorias recentes na VPN IPSec simplificam a configuração de política de firewall para conectividade VPN. A Interface de Túnel Virtual (VTI - Virtual Tunnel Interface) IPSec e o GRE+IPSec permitem o confinamento de conexões de site a site e de cliente VPN a uma zona de segurança específica colocando as interfaces de túnel em uma zona de segurança específica. As conexões poderão ser isoladas em um DMZ de VPN se a conectividade precisar ser limitada por uma política específica. Ou, se a conectividade de VPN for implicitamente confiável, ela poderá ser colocada na mesma zona de segurança que a rede interna confiável.

Se um IPSec não VTI for aplicado, a política de firewall de conectividade VPN exigirá uma análise mais cuidadosa para manter a segurança. A política de zona deve permitir especificamente o acesso por um endereço IP para hosts de local remoto ou clientes VPN se os hosts seguros estiverem em uma zona diferente da conexão criptografada do cliente VPN para o roteador. Se a política de acesso não estiver configurada corretamente, os hosts que devem ser protegidos podem acabar expostos a hosts indesejados e potencialmente hostis. Consulte Uso de VPN com firewall de política de acordo com a zona para obter mais informações sobre o conceito e a configuração.

Configuração de linguagem de política da Cisco (CPL)

Esse procedimento pode ser usado para configurar um ZFW. A sequência de etapas não é importante, mas alguns eventos devem ser concluídos na ordem. Por exemplo, configure um class-map antes de atribuí-lo a um policy-map. Da mesma forma, você não pode atribuir um policy-map a um zone-pair, até que tenha configurado a política. Se você tentar configurar uma seção que depende de outra parte da configuração não definida, o roteador responderá com uma mensagem de erro.

1. Defina zonas.
2. Defina zone-pairs.

3. Defina os class-maps que descrevem o tráfego que deve receber a política, à medida que atravessa um zone-pair.
4. Defina mapas de política para aplicar ação ao tráfego dos mapas de classe.
5. Aplique os policy-maps aos zone-pairs.
6. Atribua interfaces a zonas.

Configurar Mapas de Classes de Firewall de Política Baseada em Zona

Os class-maps definem o tráfego que o firewall seleciona para a aplicação da política. Os class-maps de Camada 4 classificam o tráfego baseado nos critérios listados aqui. Estes critérios são especificados com o comando match em um mapa de classes:

- Access-group — Uma ACL padrão, estendida ou nomeada pode filtrar o tráfego com base no endereço IP de origem e destino e na porta de origem e destino.
- Protocolo — Os protocolos da Camada 4 (TCP, UDP e ICMP) e serviços de aplicativos como HTTP, SMTP, DNS etc. Qualquer serviço conhecido ou definido pelo usuário conhecido pelo Mapeamento de Aplicativo de Porta pode ser especificado.
- Class-map — Um class-map subordinado que fornece critérios de correspondência adicionais podem ser aninhados dentro de outro class-map.
- Not — O critério not especifica que qualquer tráfego que não corresponda a um serviço especificado (protocolo), grupo de acesso ou mapa de classe subordinado será selecionado para o mapa de classe.

Combinar Critérios de "Correspondência": "Correspondência-qualquer" versus "correspondência"

Os class-maps podem aplicar operadores match-any ou match-all para determinar como aplicar os critérios de correspondência. Se match-any for especificado, o tráfego deverá atender apenas a um dos critérios de correspondência no mapa de classes. Se match-all for especificado, o tráfego deverá corresponder a todos os critérios de mapa de classe para pertencer a essa classe específica.

Critérios de correspondência devem ser aplicados a fim de mais específico para menos específico se o tráfego atender a vários critérios. Por exemplo, considere este class-map:

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

O tráfego HTTP deve encontrar o protocolo de correspondência http primeiro para garantir que o tráfego seja tratado pelos recursos específicos de serviço de inspeção de HTTP. Se as linhas de correspondência forem invertidas, o tráfego encontrará a instrução TCP do protocolo de correspondência antes de compará-la ao protocolo http, o tráfego é simplesmente classificado como tráfego TCP e inspecionado com base nas capacidades do componente Firewall TCP Inspection. Esse é um problema para determinados serviços (como FTP, TFTP) e vários serviços de sinalização de voz e multimídia (como H.323, SIP, Skinny, RTSP e outros). Esses serviços exigem recursos adicionais de inspeção para reconhecer as atividades mais complexas deles.

Aplicar uma ACL como critério de correspondência

Class-maps podem aplicar uma ACL como um dos critérios de correspondência para a aplicação

da política. Se um mapa de classe corresponder apenas ao critério de uma ACL e o mapa de classe estiver associado a um mapa de política que aplica a ação de inspeção, o roteador aplicará a inspeção básica de TCP ou UDP para todo o tráfego permitido pela ACL, exceto pelo que o ZFW fornece a inspeção com reconhecimento de aplicativos. Isso inclui (mas não se limita a) FTP, SIP, Skinny (SCCP), H.323, Sun RPC e TFTP. Se a inspeção específica da aplicação estiver disponível e a ACL permitir o canal primário ou de controle, qualquer canal secundário ou de mídia associado ao primário/controle será permitido, independentemente de a ACL permitir o tráfego.

Se um class-map aplica somente a ACL 101 como critério de correspondência, uma ACL 101 é exibida da seguinte forma:

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

Todo o tráfego é permitido na direção da política de serviço aplicada a um determinado par de zonas, e o tráfego de retorno que corresponde a isso é permitido na direção oposta. Portanto, a ACL deve aplicar a restrição para limitar o tráfego aos tipos desejados específicos. Observe que a lista PAM inclui serviços de aplicativos como HTTP, NetBIOS, H.323 e DNS. No entanto, apesar do conhecimento do PAM sobre o uso de aplicativos específicos de uma determinada porta, o firewall aplica apenas recursos suficientes específicos de aplicativos para acomodar os requisitos bem conhecidos do tráfego de aplicativos. Assim, o tráfego de aplicações simples, como Telnet, SSH, e outras aplicações de canal único, são inspecionados como TCP, e suas estatísticas são combinadas na saída do comando show. Se a visibilidade específica do aplicativo na atividade da rede for desejada, você precisará configurar a inspeção de serviços por nome do aplicativo (configurar match protocol HTTP, match protocol telnet, etc.).

Compare as estatísticas disponíveis na saída do comando show policy-map type inspect zone-pair desta configuração com a diretiva de firewall mais explícita exibida mais adiante na página. Essa configuração é usada para inspecionar o tráfego de um telefone IP Cisco, bem como várias estações de trabalho que usam uma variedade de tráfego, incluindo http, ftp, netbios, ssh e 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
```

Embora essa configuração seja fácil de definir e acomodar todo o tráfego originado na zona privada (desde que o tráfego siga as portas de destino reconhecidas por PAM padrão), ela fornece visibilidade limitada na atividade de serviço e não oferece a oportunidade de aplicar

limites de largura de banda e de sessão de ZFW para tipos específicos de tráfego. Esta saída de comando show policy-map type inspect zone-pair priv-pub é o resultado de uma configuração simples anterior que usa somente um permit ip [subnet] de qualquer ACL entre pares de zonas. Como você pode ver, a maior parte do tráfego da estação de trabalho é contabilizada nas estatísticas básicas de TCP ou UDP:

```
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
```

Por outro lado, uma configuração semelhante que adiciona classes específicas de aplicativos fornece estatísticas e controle de aplicativos mais granulares e ainda acomoda a mesma amplitude de serviços mostrada no primeiro exemplo quando você define o mapa de classes de última oportunidade que corresponde apenas à ACL como a última chance no mapa de políticas:

```
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
```

A configuração mais específica fornece essa saída granular considerável do comando show policy-map type inspect zone-pair priv-pub:

```
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
```

Outro benefício adicional quando uma configuração de mapa de classe e mapa de política mais granular é usada, como mencionado anteriormente, é uma oportunidade de aplicar limites específicos de classe em valores de sessão e taxa; e, para ajustar especificamente os parâmetros de inspeção pela aplicação de um mapa de parâmetros para ajustar cada comportamento de inspeção de classe.

Configurar Mapas de Políticas de Firewall da Política Baseada em Zona

O mapa de políticas aplica ações de política de firewall a um ou mais mapas de classe para definir a política de serviço que é aplicada a um par de zonas de segurança. Quando um inspect-type policy-map é criado, uma classe padrão denominada class class-default é aplicada no final da classe. A ação de política padrão classe-padrão é descartar, mas pode ser alterada para passar. A opção de registro pode ser adicionada com a ação de descartar. A inspeção não pode ser aplicada em class class-default.

Ações de firewall de política de acordo com a zona

O ZFW fornece três ações de tráfego que atravessam de uma zona a outra:

- Drop — Esta é a ação padrão para todo o tráfego, conforme aplicado pela classe class-default, que termina cada mapa de política do tipo inspect. Outros class-maps em um policy-map também podem ser configurados para descartar o tráfego indesejado. O tráfego que é tratado pela ação de queda é descartado silenciosamente (isto é, nenhuma notificação de queda é enviada ao host final relevante) pelo ZFW, ao contrário de um comportamento da ACL quando ele envia uma mensagem de "host inalcançável" do ICMP ao host que enviou o tráfego negado. Atualmente, não há uma opção para alterar o comportamento de queda silenciosa. A opção de registro pode ser adicionada com o descarte para notificação de syslog de que o tráfego foi descartado pelo firewall.
- Aprovar — essa ação permite que o roteador encaminhe o tráfego de uma zona até a outra. A ação de aprovação não rastreia o estado das conexões ou das sessões no tráfego. A aprovação permite apenas o tráfego em uma direção. Uma política paralela deve ser aplicada para permitir que o tráfego de retorno passe na direção oposta. A ação de aprovação é útil para protocolos ESP IPSec, IPSec AH, ISAKMP e outros protocolos inerentemente seguros com comportamento previsível. No entanto, a maior parte do tráfego de aplicações é melhor tratada no ZFW com a ação de inspeção.
- Inspecionar — a ação de inspeção oferece controle de tráfego de acordo com o estado. Por exemplo, se o tráfego da zona privada para a zona da Internet na rede de exemplo anterior for inspecionado, o roteador manterá as informações de conexão ou de sessão para o tráfego de TCP e de UDP (User Datagram Protocol). Portanto, o roteador permite o tráfego de retorno enviado de hosts de zona de Internet em resposta às solicitações de conexão de zona privada. Além disso, o Inspect pode fornecer inspeção e controle de aplicativos para determinados protocolos de serviço que podem transportar tráfego de aplicativos vulnerável

ou sensível. Audit-trail pode ser aplicada com um mapa de parâmetros para registrar a conexão/sessão iniciada, a interrupção, a duração, o volume de dados transferidos e os endereços de origem e destino.

As ações são associadas com class-maps em policy-maps:

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

Os mapas de parâmetros oferecem opções para modificar os parâmetros de conexão para uma determinada política de inspeção de mapa de classes.

Configurar mapas de parâmetros do firewall de política de zona

Os mapas de parâmetros especificam o comportamento de inspeção para ZFW, para parâmetros como proteção DoS, temporizadores de conexão TCP/UDP e configuração de registro de trilha de auditoria. Os parameter-maps também são aplicados à classe de Camada 7 e aos policy-maps para definir o comportamento específico da aplicação, como objetos HTTP, requisitos de autenticação de POP3 e IMAP e outras informações específicas da aplicação.

Os parameter-maps de inspeção para ZFW são configurados como type inspect, semelhante a outra classe de ZFW e policy-objects:

```
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
```

Os tipos específicos de parameter-maps especificam os parâmetros aplicados pelas políticas de inspeção de aplicação da camada 7. Os mapas de parâmetros do tipo Regex definem uma expressão regular para uso com a inspeção de aplicativos HTTP que filtra o tráfego com uma expressão regular:

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

Os mapas de parâmetros do tipo info do protocolo definem nomes de servidor para uso com a inspeção de aplicativos IM:

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

Detalhes completos de configuração para inspeção de aplicações HTTP e IM são fornecidos nas respectivas seções de inspeção de aplicações deste documento.

Aplicar log para políticas de firewall de política baseada em zona

O ZFW oferece opções de registro para o tráfego descartado ou inspecionado por padrão, ou para ações de política de firewall configuradas. O registro de audit-trail está disponível para o tráfego que o ZFW inspeciona. A trilha de auditoria é aplicada quando uma trilha de auditoria é definida em um mapa de parâmetros e o mapa de parâmetros com a ação de inspeção é aplicado em um mapa de políticas:

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

O registro de descarte está disponível para o tráfego que o ZFW descarta. O log de descarte é configurado pelo quando você adiciona um log com a ação de descarte em um mapa de políticas:

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

Editar mapas de classe e mapas de política do firewall de política de zona

O ZFW não incorpora atualmente um editor que possa modificar as várias estruturas de ZFW, como policy-maps, class-maps e parameter-maps. Para reorganizar as instruções de correspondência em uma aplicação de class-map ou ação para vários class-maps contidos em um policy-map, você precisa concluir estas etapas:

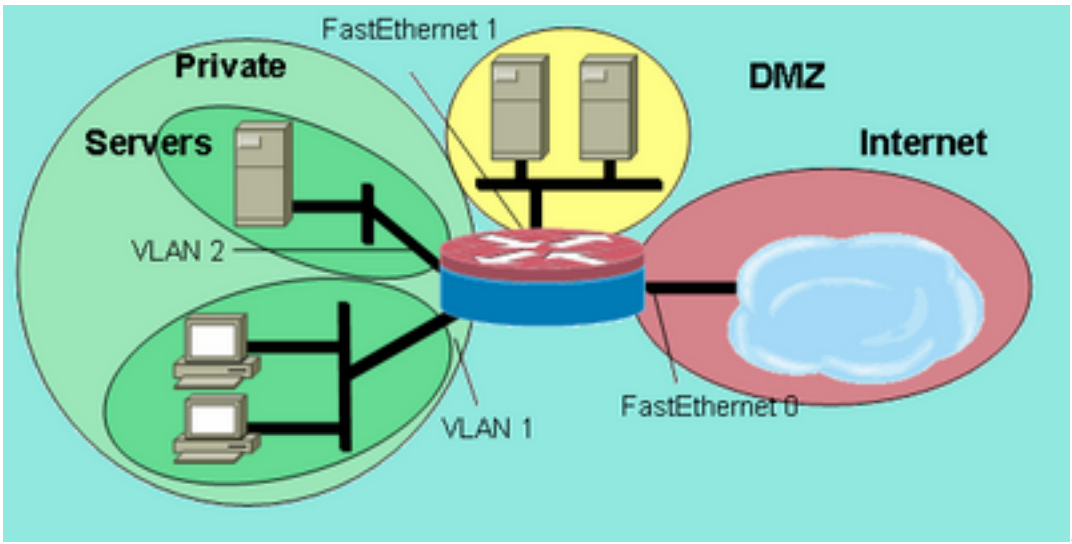
1. Copie a estrutura atual para um editor de texto, como o Bloco de Notas do Microsoft Windows, ou para um editor, como vi, em plataformas Linux/Unix.
2. Remova a estrutura atual da configuração do roteador.
3. Edite a estrutura no editor de texto.
4. Copie a estrutura de volta para a CLI do roteador.

Exemplos de configuração

Este exemplo de configuração emprega um Cisco 1811 Integrated Services Router. Uma configuração básica com conectividade IP, configuração de VLAN e ponte transparente entre dois segmentos de LAN Ethernet privados está disponível no Apêndice A. O roteador está separado em cinco zonas:

- A Internet pública está conectada à FastEthernet 0 (zona de Internet)
- Dois servidores de Internet estão conectados à FastEthernet 1 (zona DMZ)
- O switch Ethernet está configurado com duas VLANs:As estações de trabalho estão conectadas à VLAN1 (zona do cliente).Os servidores estão conectados ao VLAN2 (zona do servidor).As zonas do cliente e do servidor estão na mesma sub-rede. Um firewall transparente é aplicado entre as zonas, de modo que as políticas entre zonas nessas duas interfaces só podem afetar o tráfego entre as zonas cliente e servidor.
- As interfaces VLAN1 e VLAN2 se comunicam com outras redes por meio da interface virtual de ponte (BVI1). Essa interface é atribuída à zona privada. (Veja a Figura 2).

Figura 2: Detalhes da topologia da zona

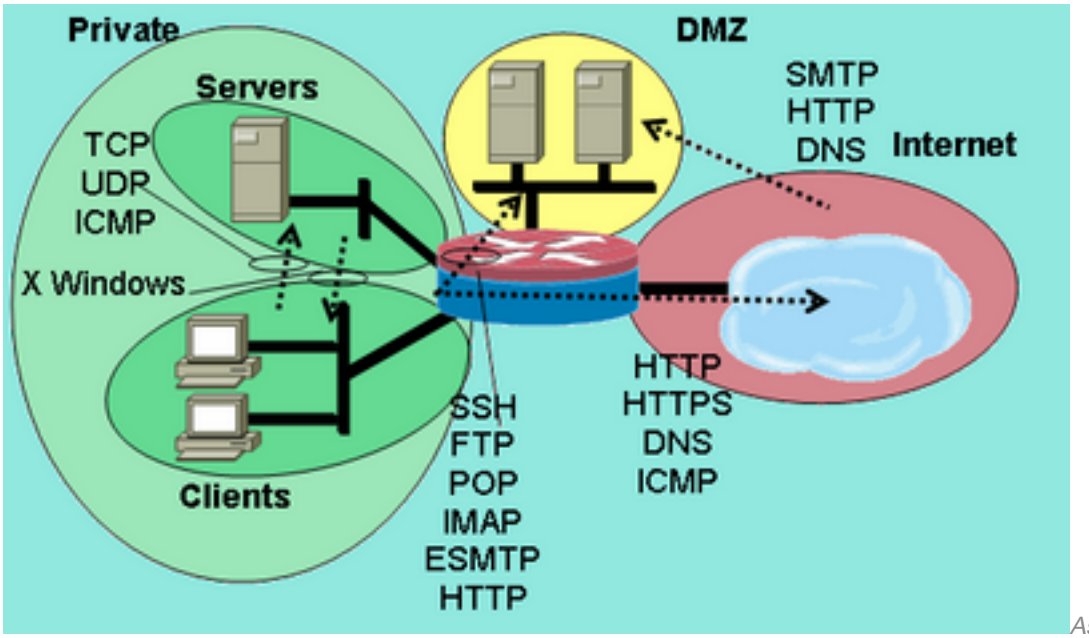


Detalhes da topologia da zona

Essas políticas são aplicadas, com as zonas de rede definidas anteriormente:

- Os hosts na zona de Internet podem acessar serviços DNS, SMTP e SSH em um servidor na DMZ. O outro servidor oferece serviços SMTP, HTTP e HTTPS. A política de firewall restringe o acesso aos serviços específicos disponíveis em cada host.
- Os hosts DMZ não podem se conectar aos hosts em nenhuma outra zona.
- Os hosts na zona do cliente podem se conectar aos hosts na zona do servidor em todos os serviços TCP, UDP e ICMP.
- Os hosts na zona do servidor não podem se conectar aos hosts na zona do cliente, exceto por um servidor de aplicações baseado em UNIX que pode abrir sessões do cliente X Windows para servidores X Windows em computadores desktop na área do cliente nas portas 6900 a 6910.
- Todos os hosts na zona privada (combinação de clientes e servidores) podem acessar os hosts em DMZ nos serviços SSH, FTP, POP, IMAP, ESMTP e HTTP e nos serviços de zona de Internet em HTTP, HTTPS e serviços DNS e ICMP. Além disso, a inspeção de aplicativos é aplicada em conexões HTTP da zona privada para a zona da Internet para garantir que aplicativos IM e P2P suportados não sejam transportados na porta 80. (Consulte a Figura 3.)

Figura 3: As permissões de serviço de zone-pair a serem aplicadas no exemplo de configuração



As permissões de serviço de zone-pair a serem aplicadas no exemplo de configuração

Essas políticas de firewall são configuradas em ordem de complexidade:

1. Inspeção de TCP/UDP/ICMP clientes-servidores
2. Inspeção de SSH/FTP/POP/IMAP/ESMTP/HTTP privada-DMZ
3. Inspeção SMTP/HTTP/DNS Internet-DMZ restrita por endereço de host
4. Inspeção X Windows de servidores-clientes com um serviço especificado por mapeamento de aplicação de porta (PAM)
5. Inspeção HTTP/HTTPS/DNS/ICMP privada-Internet com aplicação HTTP

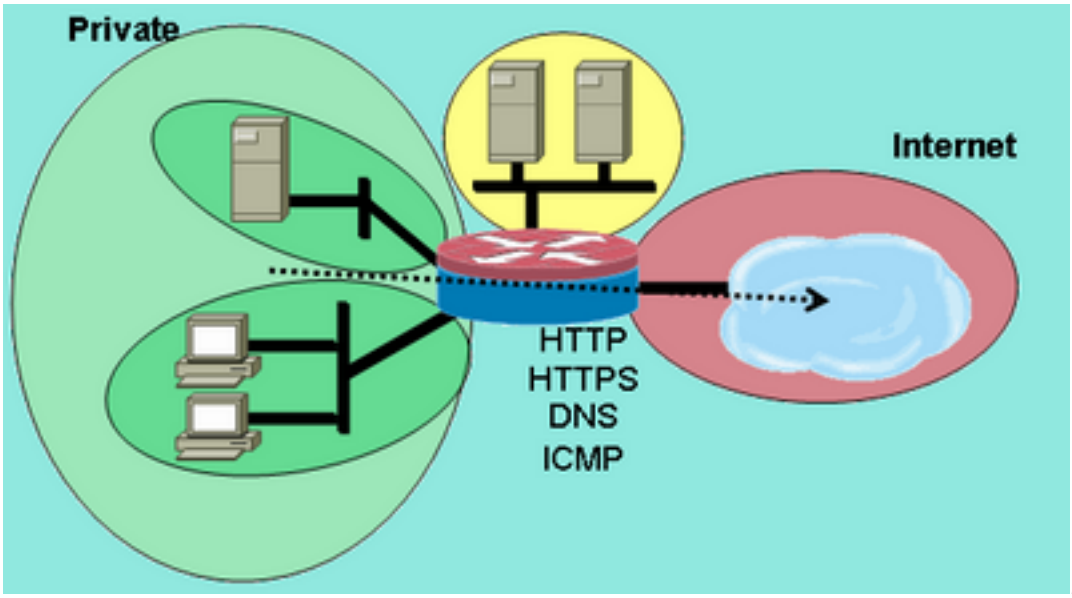
Como você aplica partes da configuração a diferentes segmentos de rede em momentos diferentes, é importante lembrar que um segmento de rede perde conectividade com outros segmentos quando é colocado em uma zona. Por exemplo, quando a zona privada é configurada, os hosts na zona privada perdem a conectividade com as zonas DMZ e Internet até que suas respectivas políticas sejam definidas.

Firewall de roteamento de inspeção stateful

Configurar política privada de Internet

A figura 4 ilustra a configuração da política de Internet privada.

Figura 4: Inspeção de serviço de zona privada para a zona da Internet



Inspeção de serviço de zona privada para a zona da Internet

A política de Internet privada aplica a inspeção de Camada 4 à inspeção de HTTP, HTTPS, DNS e Camada 4 para ICMP, da zona privada até a zona da Internet. Isso permite conexões da zona privada com a zona da Internet e permite o tráfego de retorno. A inspeção da camada 7 traz as vantagens de um controle mais rígido do aplicativo, melhor segurança e suporte para aplicativos que exigem correção. No entanto, a inspeção da Camada 7, como mencionado, requer um melhor entendimento da atividade da rede, já que os protocolos da Camada 7 que não estão configurados para inspeção não são permitidos entre zonas.

1. Defina mapas de classe que descrevam o tráfego que você deseja permitir entre regiões, com base nas políticas descritas anteriormente:
```
configure terminal
 class-map type inspect match-any internet-traffic-class
  match protocol http
  match protocol https
  match protocol dns
  match protocol icmp
```
2. Configure um policy-map para inspecionar o tráfego nos class-maps que você acabou de definir:
```
configure terminal
 policy-map type inspect private-internet-policy
  class type inspect internet-traffic-class
   inspect
```
3. Configure as zonas de Internet e privadas e atribua interfaces de roteador às suas respectivas zonas:
```
configure terminal
 zone security private
 zone security internet
 int bvi1
  zone-member security private
 int fastethernet 0
  zone-member security internet
```

Configure o zone-pair e aplique o policy-map apropriado.

> **Note**: Você só precisa configurar o par de zona de Internet privada no momento para inspecionar conexões originadas na zona privada que viaja para a zona de Internet, mostrada a seguir:

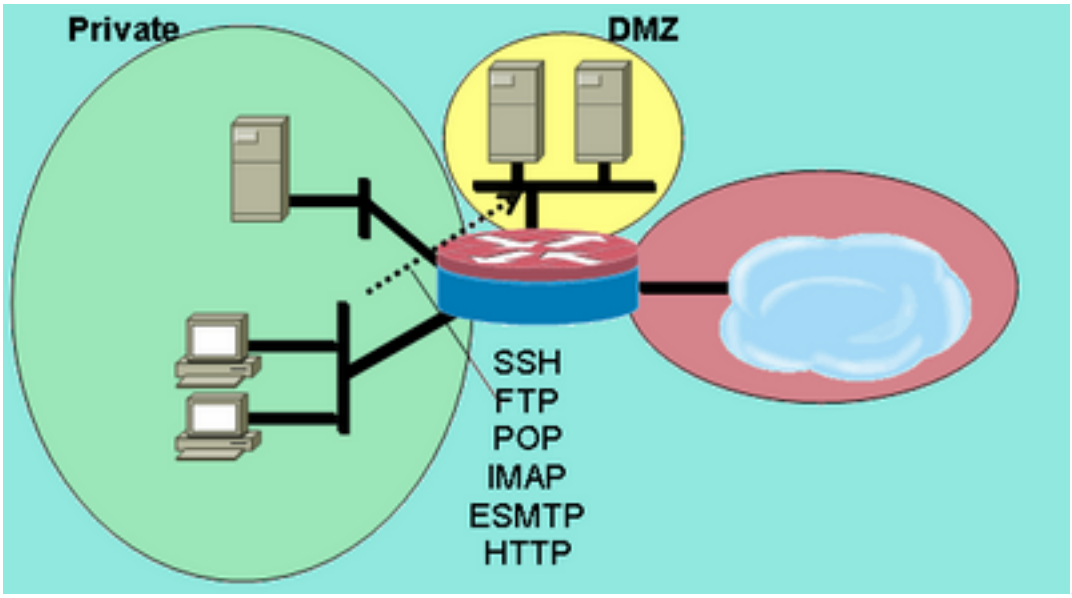
```
configure terminal
 zone-pair security private-internet source private destination internet
  service-policy type inspect private-internet-policy
```

Isso conclui a configuração da política de inspeção da Camada 7 no par de zonas da Internet privada para permitir conexões HTTP, HTTPS, DNS e ICMP da zona de clientes para a zona de servidores e aplicar inspeção de aplicações ao tráfego HTTP e garantir que a passagem do tráfego indesejado não seja permitido na porta de serviço do HTTP, TCP 80.

Configurar a política DMZ privada

A figura 5 ilustra a configuração da política de DMZ privada.

Figura 5: Inspeção de serviço de zona privada para a zona de DMZ



Inspeção de serviço de zona privada para a zona de DMZ

A política de DMZ privada traz mais complexidade, pois requer uma melhor compreensão do tráfego de rede entre as zonas. Essa política aplica a inspeção de Camada 7 da zona privada para a DMZ. Isso permite conexões da zona privada para a DMZ e permite o tráfego de retorno. A inspeção da camada 7 traz as vantagens de um controle mais rígido do aplicativo, melhor segurança e suporte para aplicativos que exigem correção. No entanto, a inspeção da Camada 7, como mencionado, requer um melhor entendimento da atividade da rede, já que os protocolos da Camada 7 que não estão configurados para inspeção não são permitidos entre zonas.

1. Defina mapas de classe que descrevam o tráfego que você deseja permitir entre regiões, com base nas políticas descritas anteriormente:
   ```
   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. Configurar policy-maps para inspecionar o tráfego nos class-maps que você acabou de definir:
   ```
   configure terminal
    policy-map type inspect private-dmz-policy
   ```

```
 class type inspect L7-inspect-class
  inspect
```

3. Configure as zonas de DMZ e privadas e atribua interfaces de roteador às suas respectivas zonas:

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

4. Configure o zone-pair e aplique o policy-map apropriado.

Note: No momento, você só precisa configurar o par de zonas DMZ privadas para inspecionar as conexões originadas na zona privada que trafega para a DMZ, mostrado a seguir:

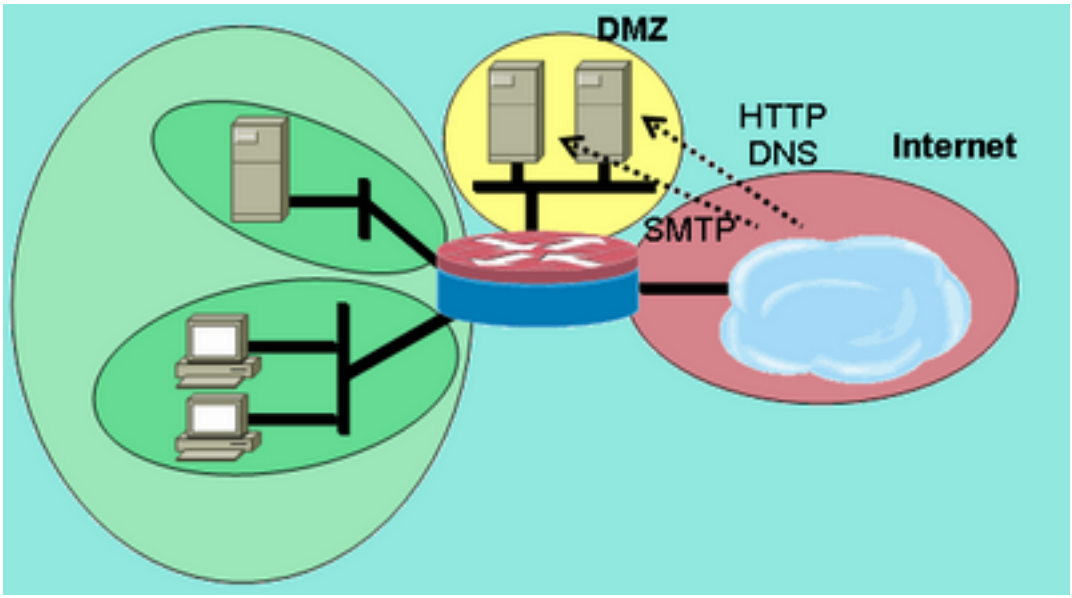
```
configure terminal
 zone-pair security private-dmz source private destination dmz
  service-policy type inspect private-dmz-policy
```

Isso conclui a configuração da política de inspeção da Camada 7 na DMZ privada para permitir todas as conexões TCP, UDP e ICMP da zona de clientes para a zona de servidores. A política não aplica correções para canais subordinados, mas fornece um exemplo de política simples para acomodar a maioria das conexões de aplicativos.

Configurar a política de DMZ de Internet

A figura 6 ilustra a configuração da política DMZ da Internet.

Figura 6: Inspeção de serviço de zona de Internet para a zona de DMZ



Inspeção de serviço de zona de Internet para a zona de DMZ

Essa política aplica a inspeção de Camada 7 da zona de Internet para a DMZ. Isso permite conexões da zona da Internet com a DMZ e permite o tráfego de retorno dos hosts da DMZ para os hosts da Internet que originaram a conexão. A política da DMZ da Internet combina a inspeção da Camada 7 com grupos de endereços definidos por ACLs, visando restringir o acesso a serviços específicos em hosts, grupos de hosts ou sub-redes específicos. Para realizar esse

aninhamento, um mapa de classe que especifica serviços em outro mapa de classe que faz referência a uma ACL para especificar endereços IP.

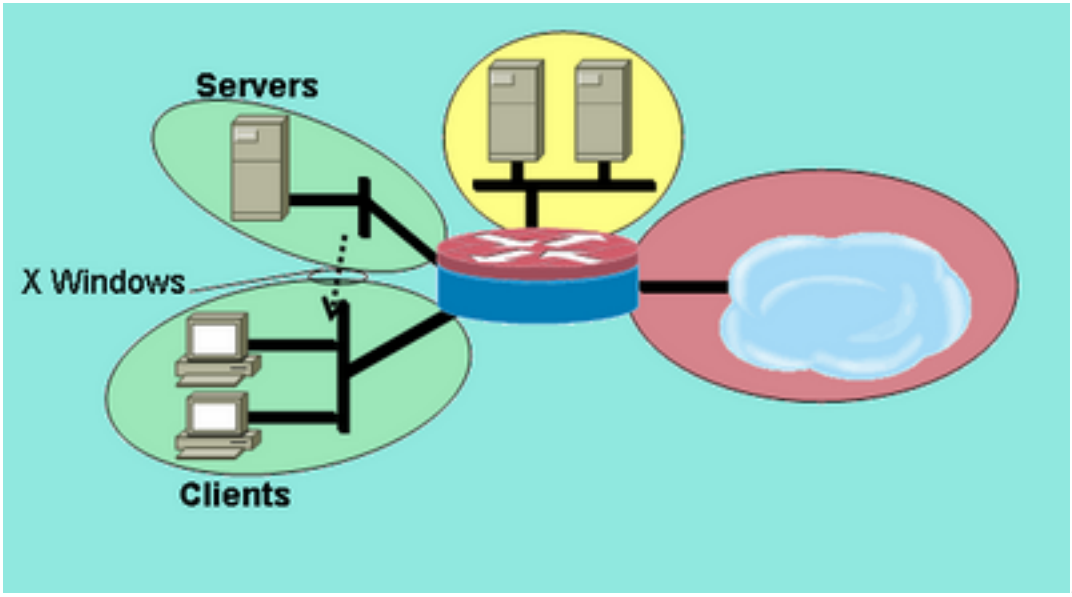
1. Defina mapas de classe e ACLs que descrevam o tráfego que você deseja permitir entre regiões, com base nas políticas descritas anteriormente.Vários mapas de classe para serviços devem ser usados, já que diferentes políticas de acesso são aplicadas para acesso a dois servidores diferentes. Os hosts de Internet têm permissão para conexões DNS e HTTP para 172.16.2.2 e as conexões SMTP têm permissão para 172.16.2.3. Observe a diferença nos mapas de classe. Os class-maps que especificam serviços usam a palavra-chave match-any para permitir qualquer um dos serviços listados. Os class-maps associando ACLs aos class-maps de serviço usam a palavra-chave match-all para exigir que ambas as condições no mapa de classe devam ser atendidas para permitir o tráfego:
```
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. Configurar policy-maps para inspecionar o tráfego nos class-maps que você acabou de definir:
```
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. Configure as zonas de DMZ e Internet e atribua interfaces de roteador às suas respectivas zonas. Ignore a configuração da DMZ, se ela for configurada na seção anterior:
```
configure terminal
zone security internet
zone security dmz
int fastethernet 0
 zone-member security internet
int fastethernet 1
 zone-member security dmz
```
4. Configure o zone-pair e aplique o policy-map apropriado.**Note**: No momento, você só precisa configurar o par de zonas DMZ da Internet para inspecionar as conexões originadas na zona da Internet que trafega para a zona DMZ, mostrada a seguir:
```
configure terminal
 zone-pair security internet-dmz source internet destination dmz
  service-policy type inspect internet-dmz-policy
```
Isso conclui a configuração da política de inspeção da Camada 7 específica do endereço no zone-pair da DMZ da Internet.

Firewall transparente de inspeção stateful

Configurar a política de servidores-clientes

A próxima figura ilustra a configuração da política servidor-cliente.

Figura 7: Inspeção de serviço da zona de Servidores para a zona de Clientes



Inspeção de serviço da zona de Servidores para a zona de Clientes

A política de servidores-clientes aplica inspeção com um serviço definido pelo usuário. A inspeção da Camada 7 é aplicada da zona de servidores à zona de clientes. Isso permite conexões X Windows a um intervalo de portas específico da zona de servidores à zona de clientes e permite o tráfego de retorno. O X Windows não é um protocolo nativo suportado no PAM, portanto um serviço configurado pelo usuário no PAM deve ser definido para que o ZFW possa reconhecer e inspecionar o tráfego apropriado.

Duas ou mais interfaces de roteador são configuradas em um grupo de pontes IEEE para fornecer Integrated Routing and Bridging (IRB) para fornecer bridging entre as interfaces no grupo de pontes e para rotear para outras sub-redes através da Bridge Virtual Interface (BVI). A política de firewall transparente aplica a inspeção de firewall para o tráfego que "atravessa a ponte", mas não para o tráfego que sai do grupo de pontes através do BVI. A política de inspeção só se aplica ao tráfego que atravessa o bridge-group. Portanto, nesse cenário, a inspeção é aplicada apenas ao tráfego que se move entre as zonas de clientes e servidores, que são aninhadas dentro da zona privada. A política aplicada entre a zona privada e as zonas pública e DMZ só entra em cena quando o tráfego deixa o grupo de pontes pelo BVI. Quando o tráfego sai via BVI das zonas de clientes ou servidores, a política de firewall transparente não é chamada.

1. Configure o PAM com uma entrada definida pelo usuário para X Windows.Os clientes X Windows (onde os aplicativos estão hospedados) abrem conexões para exibir informações aos clientes (onde o usuário trabalha) em um intervalo que começa na porta 6900.Cada conexão adicional usa portas sucessivas, portanto, se um cliente exibir 10 sessões diferentes em um host, o servidor usará as portas 6900-6909. Portanto, se você inspecionar o intervalo de portas de 6900 a 6909, as conexões abertas para portas além de 6909 falharão:
   ```
   configure terminal
    ip port-map user-Xwindows port tcp from 6900 to 6910
   ```
2. Revise os documentos do PAM para abordar outras perguntas sobre o PAM ou verificar a documentação da inspeção de protocolo granular para obter informações sobre os detalhes de interoperabilidade entre o PAM e a inspeção stateful do Cisco IOS Firewall.
3. Defina mapas de classe que descrevam o tráfego que você deseja permitir entre regiões,

com base nas políticas descritas anteriormente:

```
configure terminal
 class-map type inspect match-any Xwindows-class
  match protocol user-Xwindows
```

4. Configurar policy-maps para inspecionar o tráfego nos class-maps que você acabou de definir:

```
configure terminal
 policy-map type inspect servers-clients-policy
  class type inspect Xwindows-class
   inspect
```

5. Configure as zonas do cliente e servidor e atribua interfaces de roteador às suas respectivas zonas.Se você configurou essas zonas e as interfaces atribuídas na seção de configuração de política clients-servers, é possível pular para a definição de zone-pair. A configuração da ponte IRB é fornecida para fins de abrangência:

```
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. Configure o zone-pair e aplique o policy-map apropriado.**Note**: Você só precisa configurar o par de zonas servidores-clientes no momento para inspecionar conexões originadas na zona de servidores que trafegam para a zona de clientes, mostrada a seguir:

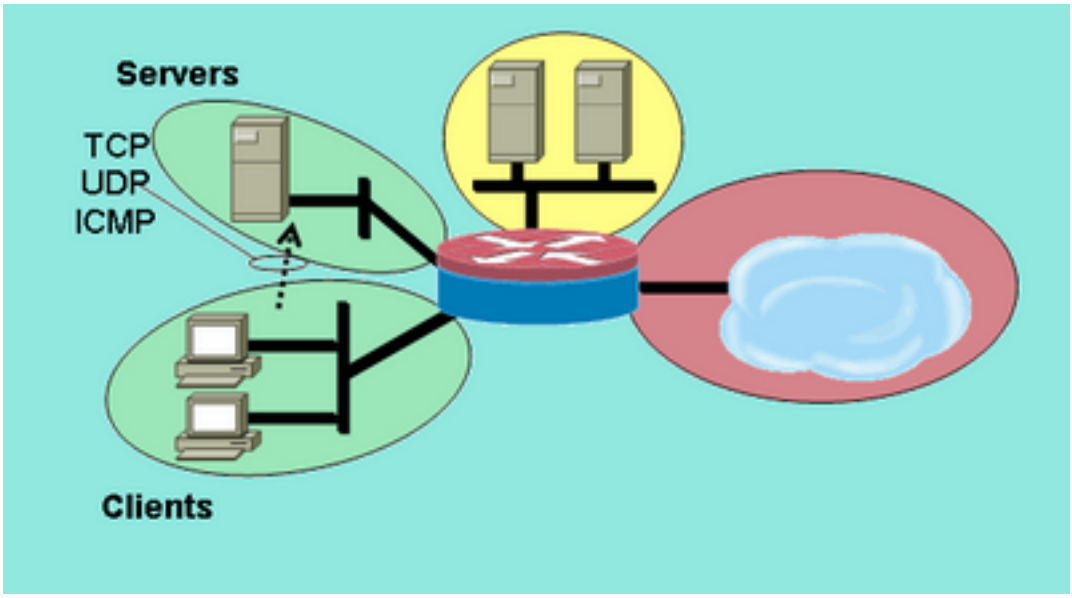
```
configure terminal
 zone-pair security servers-clients source servers destination clients
  service-policy type inspect servers-clients-policy
```

Isso conclui a configuração da política de inspeção definida pelo usuário no zone-pair servidores-clientes para permitir conexões X Windows da zona do servidor para a zona do cliente.

Configurar a política de clients-servers

A Figura 8 ilustra a configuração da política de client-server.

Figura 8: Inspeção de serviço da zona de Clientes para a zona de Servidores



Inspeção de serviço da zona de Clientes para a zona de Servidores

A política de cliente-servidores é menos complexa do que as outras. A inspeção da Camada 4 é aplicada da zona de clientes à zona de servidores. Isso permite conexões da zona de clientes para a zona de servidores e permite tráfego de retorno. A inspeção da Camada 4 traz simplifica a configuração do firewall, pois são necessárias apenas algumas regras para permitir a maior parte do tráfego de aplicações. No entanto, a inspeção da Camada 4 também tem duas desvantagens principais:

- Aplicativos como FTP ou serviços de mídia frequentemente negociam um canal subordinado adicional do servidor para o cliente. Essa funcionalidade geralmente é acomodada em uma correção de serviço que monitora o diálogo do canal de controle e permite o canal subordinado. Esse recurso não está disponível na inspeção da Camada 4.
- A inspeção da Camada 4 permite quase todo o tráfego da camada de aplicação. Se o uso da rede precisar ser controlado para que apenas algumas aplicações sejam permitidas pelo firewall, uma ACL deverá ser configurada no tráfego de saída para limitar os serviços permitidos pelo firewall.

As duas interfaces do roteador são configuradas em um grupo de pontes IEEE, portanto, essa política de firewall aplica inspeção de firewall transparente. Essa política é aplicada em duas interfaces em um grupo de ponte de IEEE. A política de inspeção aplica-se apenas ao tráfego que atravessa o grupo de bridge. Isso explica por que as zonas clientes e servidores estão aninhadas dentro da zona privada.

1. Defina mapas de classe que descrevam o tráfego que você deseja permitir entre regiões, com base nas políticas descritas anteriormente:
```
configure terminal
 class-map type inspect match-any L4-inspect-class
 match protocol tcp
 match protocol udp
 match protocol icmp
```
2. Configurar policy-maps para inspecionar o tráfego nos class-maps que você acabou de definir:
```
configure terminal
 policy-map type inspect clients-servers-policy
 class type inspect L4-inspect-class
  inspect
```
3. Configure as zonas de clientes e servidores e atribua interfaces de roteador às suas respectivas zonas:

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

4. Configure o zone-pair e aplique o policy-map apropriado.**Note**: Você só precisa configurar o par de zonas clientes-servidores no momento para inspecionar conexões originadas na zona de clientes que viajam para a zona de servidores, mostrada a seguir:

```
configure terminal
 zone-pair security clients-servers source clients destination servers
  service-policy type inspect clients-servers-policy
```

Isso conclui a configuração da política de inspeção da Camada 4 de clients-servers zone-pair para permitir todas as conexões TCP, UDP e ICMP da zona de cliente para a zona de servidor. A política não aplica correções para canais subordinados, mas fornece um exemplo de política simples para acomodar a maioria das conexões de aplicativos.

Política de Taxa para Firewall de Política Baseada em Zona

As redes de dados frequentemente se beneficiam com a capacidade de limitar a taxa de transmissão de tipos específicos de tráfego de rede e de limitar o impacto do tráfego de prioridade mais baixa a um tráfego essencial para a empresa. O software Cisco IOS oferece esse recurso com vigilância de tráfego , que limita a taxa nominal de tráfego e o burst. O software Cisco IOS tem a política de tráfego compatível desde o Cisco IOS versão 12.1(5)T.

O Cisco IOS Software Release 12.4(9)T aumenta o ZFW com limitação de taxa quando você adiciona a capacidade de policiar o tráfego que se aplica que corresponde às definições de um mapa de classe específico quando ele atravessa o firewall de uma zona de segurança para outra. Isso oferece a conveniência de um ponto de configuração para descrever o tráfego específico, aplicar a política de firewall e vigiar esse consumo de largura de banda de tráfego. O ZFW difere do baseado em interface porque fornece apenas as ações de transmissão para conformidade de política e queda para violação de política. O ZFW não pode marcar o tráfego para DSCP.

O ZFW só pode especificar o uso de largura de banda em bytes/segundo, pacote/segundo e a porcentagem de largura de banda não é oferecida. O ZFW pode ser aplicado com ou sem interface-based. Portanto, se forem necessários recursos adicionais, esses recursos podem ser aplicados por interface baseada em. Se o baseado em interface for usado em conjunto com o firewall, certifique-se de que as políticas não entrem em conflito.

Configurar política ZFW

O policiamento de ZFW limita o tráfego em um mapa de classe de política a um valor de taxa definido pelo usuário entre 8.000 e 2.000.000.000 bits por segundo, com um valor de burst configurável no intervalo de 1.000 a 512.000.000 bytes.

A política de ZFW é configurada por uma linha adicional de configuração em policy-map, que é aplicada após a ação da política:

```
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>]
```

Controle de sessão

A política de ZFW também introduziu o controle de sessão para limitar a contagem de sessão para tráfego em um mapa de política que se aplica que corresponda a um mapa de classe. Isso aumenta a capacidade atual de aplicar a política de proteção contra DoS por mapa de classe. Efetivamente, isso permite o controle granular do número de sessões que se aplicam que corresponde a qualquer mapa de classe fornecido que atravessa um par de zonas. Se o mesmo class-map é usado em vários policy-maps ou zone-pairs, os limites de sessão diferentes podem ser aplicados em vários aplicações de class-map.

O controle de sessão é aplicado quando um mapa de parâmetros é configurado e contém o volume de sessão desejado, e o mapa de parâmetros é anexado à ação de inspeção aplicada a um mapa de classes em um mapa de políticas:

```
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
```

Os mapas de parâmetros só podem ser aplicados à ação de inspeção e não estão disponíveis em ações de aprovação ou soltar.

As atividades de controle e vigilância de sessão ZFW são visíveis com este comando:

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

Inspeção de aplicações

A inspeção de aplicações introduz recursos adicionais para o ZFW. As políticas de inspeção de aplicação são aplicadas na Camada 7 do modelo OSI, onde as aplicações do usuário enviam e recebem mensagens que permitem às aplicações oferecerem recursos úteis. Alguns aplicativos podem oferecer recursos indesejados ou vulneráveis, portanto, as mensagens associadas a esses recursos devem ser filtradas para limitar as atividades nos serviços de aplicativos.

O ZFW do software Cisco IOS oferece inspeção e controle de aplicações nesses serviços de aplicações:

- HTTP
- SMTP
- POP3
- IMAP
- RPC da Sun
- Tráfego de aplicação P2P
- Aplicações de IM

A inspeção e o controle de aplicações (AIC) variam de acordo com a capacidade por serviço. A inspeção de HTTP oferece filtragem granular em vários tipos de atividade de aplicativos e fornece recursos para limitar o tamanho da transferência, o tamanho do endereço da Web e a atividade do navegador para impor conformidade com padrões de comportamento de aplicativos e para

limitar os tipos de conteúdo que são transferidos pelo serviço. O AIC para SMTP pode limitar o tamanho do conteúdo e reforçar a conformidade do protocolo. A inspeção POP3 e IMAP pode ajudar a garantir que os usuários usem mecanismos de autenticação seguros para evitar o comprometimento das credenciais do usuário.

A inspeção de aplicativos é configurada como um conjunto adicional de mapas de classe e mapas de política específicos do aplicativo, que são então aplicados aos mapas de classe e mapas de política de inspeção atuais quando você define a política de serviço do aplicativo no mapa de política de inspeção.

Inspeção de aplicações HTTP

A inspeção de aplicativos pode ser aplicada no tráfego HTTP para controlar o uso indesejado da porta de serviço HTTP para outros aplicativos, como IM, compartilhamento de arquivos P2P e aplicativos de tunelamento que podem redirecionar aplicativos que, de outra forma, teriam firewall por meio do TCP 80.

Configure um class-map de inspeção de aplicação para descrever o tráfego que viola o tráfego HTTP permitido:

```
! 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
```

Melhorias na inspeção de aplicações HTTP

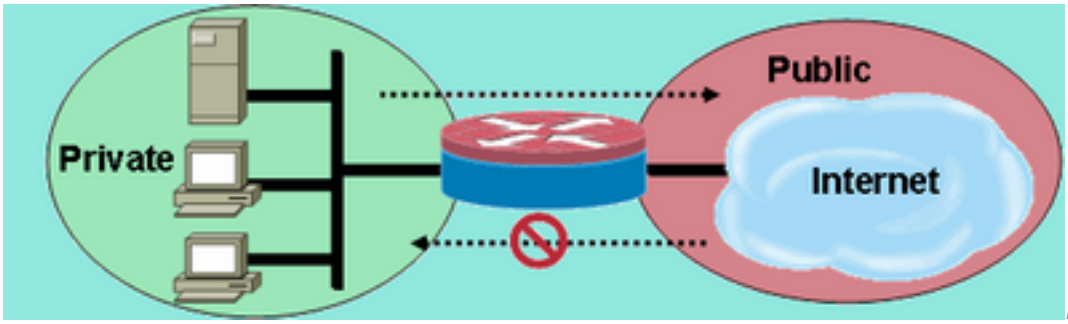
O Cisco IOS Software Release 12.4(9)T introduz melhorias nos recursos de inspeção de HTTP do ZFW. O firewall Cisco IOS introduziu a inspeção de aplicação HTTP no software Cisco IOS versão 12.3(14)T. O Cisco IOS Software Release 12.4(9)T aumenta as capacidades atuais quando você adiciona:

- Capacidade de permitir, negar e monitorar solicitações e respostas com base nos valores de nome e cabeçalho do cabeçalho. Isso é útil para bloquear solicitações e respostas que transportam campos de cabeçalho vulneráveis.

- Capacidade de limitar os tamanhos de diferentes elementos nos cabeçalhos de solicitação e resposta HTTP, como o comprimento máximo da URL, o comprimento máximo do cabeçalho, o número máximo de cabeçalhos, o comprimento máximo da linha do cabeçalho e assim por diante. Isso é útil para evitar estouros de buffer.
- Capacidade de bloquear solicitações e respostas que transportam vários cabeçalhos do mesmo tipo; por exemplo, uma solicitação com dois cabeçalhos de tamanho de conteúdo.
- Capacidade de bloquear solicitações e respostas com cabeçalhos não ASCII. Isso é útil para evitar vários ataques que usam binários e outros caracteres não ASCII para introduzir worms e outros conteúdos mal-intencionados em servidores da Web.
- Éoferecida a capacidade de agrupar métodos HTTP em categorias e flexibilidade especificadas pelo usuário para bloquear/permitir/monitorar cada um dos grupos. O RFC HTTP permite um conjunto restrito de métodos HTTP. Alguns métodos padrão são considerados não seguros, pois podem ser usados para explorar vulnerabilidades em um servidor da Web. Muitos métodos fora do padrão têm um registro de segurança ineficiente.
- O método para bloquear URIs específicos de acordo com uma expressão regular configurada pelo usuário. Esse recurso permite que um usuário bloqueie consultas e URI personalizados.
- Capacidade de falsificar tipos de cabeçalho (especialmente o tipo de cabeçalho do servidor) com sequências de caracteres personalizáveis pelo usuário. Isso é útil quando um invasor analisa as respostas do servidor da Web e aprende o máximo de informações possível e, em seguida, inicia um ataque que explora os pontos fracos nesse servidor da Web específico.
- Capacidade de bloquear ou emitir um alerta em uma conexão HTTP se um ou mais valores de parâmetros HTTP corresponderem a valores inseridos pelo usuário como uma expressão regular. Alguns dos possíveis contextos de valor HTTP incluem o cabeçalho, o corpo, o nome de usuário, a senha, o agente de usuário, a linha de solicitação, a linha de status e as variáveis CGI decodificadas.

Exemplos de configuração para melhorias na inspeção de aplicativos HTTP supõem uma rede simples, como mostrado na Figura 9.

Figura 9: Inspeção de aplicativos Presume uma rede simples



Inspeção de aplicativos Presume uma rede simples

O firewall agrupa o tráfego em duas classes:

- Tráfego HTTP
- Todos os outros tráfegos TCP, UDP e ICMP de canal único

O HTTP é separado para permitir a inspeção específica no tráfego da Web. Isso permite que você configure a vigilância na primeira seção deste documento e a inspeção do aplicação de HTTP na segunda seção. Você pode configurar mapas de classe e mapas de política específicos para o tráfego P2P e IM na terceira seção deste documento. A conectividade é permitida da zona privada para a zona pública. Nenhuma conectividade é fornecida da zona pública para a zona privada.

Consulte o Apêndice C para obter uma configuração completa que implementa a política inicial.

Configurar Melhorias da Inspeção de Aplicativos HTTP

A inspeção de aplicações HTTP (bem como outras políticas de inspeção de aplicações) requer configurações mais complexas que a configuração básica da Camada 4. Você deve configurar a classificação e a política de tráfego da Camada 7 para reconhecer o tráfego específico que deseja controlar e aplicar a ação desejada a tráfegos desejáveis e indesejados.

A inspeção de aplicações HTTP (semelhante a outros tipos de inspeção de aplicações) só pode ser aplicada ao tráfego HTTP. Portanto, você deve definir class-maps e policy-maps de Camada 7 para tráfego HTTP específico, depois definir um class-map de Camada 4 especificamente para HTTP e aplicar a política de Camada 7 à inspeção HTTP em um policy-map de Camada 4, dessa forma:

```
!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
```

Todas essas características de tráfego de inspeção do aplicação HTTP são definidas em um class-map de Camada 7:

- O comando de inspeção de cabeçalho permite permitir/negar/monitorar solicitações ou respostas cujo cabeçalho corresponda à expressão regular configurada. A ação permitir ou redefinir pode ser aplicada a uma solicitação ou resposta que corresponda aos critérios de mapa de classe. A adição da ação de registro causa uma mensagem syslog: `APPFW-6-HTTP_HDR_REGEX_MATCHED`
  Uso do comando:

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

Exemplos de casos de uso

- Configure uma política http appfw para bloquear a solicitação ou a resposta cujo cabeçalho contém caracteres não ASCII.

```
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
```

Header length inspection — Esse comando verifica o tamanho de um cabeçalho de solicitação ou de resposta e aplica a ação se o tamanho exceder o limite configurado. Ação permitida ou redefinida. A adição da ação de registro causa uma mensagem syslog:

```
APPFW-4- HTTP_HEADER_LENGTH
```

Uso do comando:

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

Exemplos de casos de uso

Configure uma política http appfw para bloquear solicitações e respostas que tenham um tamanho de cabeçalho superior a 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
```

Header count inspection — Esse comando verifica o número de linhas de cabeçalho (campos) em uma solicitação/resposta e aplica uma ação quando a contagem excede o limite configurado. Ação permitida ou redefinida. A adição da ação de registro causa uma mensagem syslog:

```
APPFW-6- HTTP_HEADER_COUNT
```

Uso do comando:

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

Exemplos de casos de uso

Configure uma política http appfw para bloquear uma solicitação com mais de 16 campos de cabeçalho.

```
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
```

Header field inspection — Esse comando permite permitir/negar/monitorar solicitações/respostas que contêm um campo e um valor de cabeçalho HTTP específico. A ação permitir ou redefinir pode ser aplicada a uma solicitação ou resposta que corresponda aos critérios de mapa de classe. A adição da ação de registro causa uma mensagem syslog:

APPFW-6- HTTP_HDR_FIELD_REGEX_MATCHED

Uso do comando:

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

Exemplos de casos de uso

Configure uma política de inspeção de aplicação http para bloquear Spyware/Adware:

```
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
```

Header field length inspection — Esse comando permite limitar o tamanho de uma linha de campo de cabeçalho. A ação permitir ou redefinir pode ser aplicada a uma solicitação ou resposta que corresponda aos critérios de mapa de classe. A adição da ação de registro causa uma mensagem syslog:

APPFW-6- HTTP_HDR_FIELD_LENGTH

Uso do comando:

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

Exemplos de casos de uso

Configure uma política http appfw para bloquear uma solicitação cujo tamanho do campo de cookie e agente de usuário exceda 256 e 128 respectivamente.

```
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
```

Inspection of header field repetition — Esse comando verifica se uma solicitação ou resposta tem campos de cabeçalho repetidos. A ação permitir ou redefinir pode ser aplicada a uma solicitação ou resposta que corresponda aos critérios de mapa de classe. Quando ativada, a ação de log

causa uma mensagem syslog:

```
APPFW-6- HTTP_REPEATED_HDR_FIELDS
```

Uso do comando:

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

Exemplos de casos de uso

Configure uma política http appfw para bloquear uma solicitação ou resposta que tenha várias linhas de cabeçalho de tamanho de conteúdo. Essa é uma das funcionalidades mais úteis usadas para impedir o contrabando de sessão .

```
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
```

- Method inspection — O RFC HTTP permite um conjunto restrito de métodos HTTP. No entanto, até mesmo alguns métodos padrão são considerados não seguros, pois podem ser usados para explorar vulnerabilidades em um servidor da Web. Muitos dos métodos fora do padrão são usados frequentemente para atividades mal-intencionadas. Isso exige uma necessidade de agrupar os métodos em várias categorias e fazer com que o usuário escolha a ação para cada categoria. Esse comando fornece ao usuário uma maneira flexível de agrupar os métodos em várias categorias, como métodos seguros, métodos não seguros, métodos webdav, métodos RFC e métodos estendidos. A ação permitir ou redefinir pode ser aplicada a uma solicitação ou resposta que corresponda aos critérios de mapa de classe. A adição da ação de registro causa uma mensagem syslog:

```
APPFW-6-HTTP_METHOD
```

Uso do comando:

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

Exemplos de casos de uso

Configure uma política de appfw http que agrupa os métodos HTTP em três categorias: seguro, não seguro e webdav. Eles são mostrados na próxima tabela. Configure as ações de modo que:

- Todos os métodos seguros sejam permitidos sem registro
- Todos os métodos não seguros sejam permitidos com o registro
- Todos os métodos webdav são bloqueados com o registro.

Solicitações	Não seguro	WebDAV
GET, HEAD, OPTION	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 — Esse comando fornece a capacidade de permitir/negar/monitorar solicitações cujo URI corresponde à inspeção regular configurada. Esse recurso possibilita que um usuário bloqueie URLs e consultas personalizadas. A ação permitir ou redefinir pode ser aplicada a uma solicitação ou resposta que corresponda aos critérios de mapa de classe. A adição da ação de registro causa uma mensagem syslog:

```
APPFW-6- HTTP_URI_REGEX_MATCHED
```

Uso do comando:

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

Exemplos de casos de uso

Configure uma política http appfw para bloquear uma solicitação cujo URI corresponda a qualquer uma destas expressões regulares:

- .* cmd. exe
- .*sex
- .*gambling

```
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
```

- Inspeção de comprimento de URI — Este comando verifica o comprimento do URI que é enviado em uma solicitação e aplica a ação configurada quando o comprimento excede o limite configurado. A ação permitir ou redefinir pode ser aplicada a uma solicitação ou

resposta que corresponda aos critérios de mapa de classe. A adição da ação de registro causa uma mensagem syslog:

```
APPFW-6- HTTP_URI_LENGTH
```

Uso do comando:

```
match request uri length gt <bytes>
```

Exemplos de casos de uso

Configure uma política http appfw para disparar um alarme sempre que o comprimento de URI de uma solicitação exceder 3076 bytes.

```
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 — Esse comando oferece uma capacidade de permitir, negar ou monitorar solicitações cujos argumentos (parâmetros) correspondem à inspeção regular configurada. A ação permitir ou redefinir pode ser aplicada a uma solicitação ou resposta que corresponda aos critérios de mapa de classe. A adição da ação de registro causa uma mensagem syslog:

```
APPFW-6- HTTP_ARG_REGEX_MATCHED
```

Uso do comando:

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

Configure uma política http appfw para bloquear uma solicitação cujos argumentos correspondam a qualquer uma destas expressões regulares:

- .*codered
- .*attack

```
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
```

- Inspeção de comprimento de argumento — Esse comando verifica o comprimento dos argumentos enviados em uma solicitação e aplica a ação configurada quando o comprimento excede o limite configurado. A ação permitir ou redefinir pode ser aplicada a uma solicitação ou resposta que corresponda aos critérios de mapa de classe. A adição da ação de registro causa uma mensagem syslog:

  ```
  APPFW-6- HTTP_ARG_LENGTH
  ```

  Uso do comando:

  ```
  match request arg length gt <bytes>
  ```

  Exemplos de casos de uso

Configure uma política http appfw para gerar um alarme sempre que o comprimento do argumento de uma solicitação exceder 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
```

- Body inspection — Essa CLI permite que o usuário especifique uma lista de expressões regulares para corresponder ao corpo da solicitação ou resposta. A ação permitir ou redefinir pode ser aplicada a uma solicitação ou resposta que corresponda aos critérios de mapa de classe. A adição da ação de registro causa uma mensagem syslog:
  `APPFW-6- HTTP_BODY_REGEX_MATCHED`
  Uso do comando:
  `match {request|response|reg-resp} body regex <parameter-map-name>`
  Exemplos de casos de uso

Configure um http appfw para bloquear uma resposta cujo corpo contenha o padrão `.*[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
```

Inspeção de comprimento do corpo (conteúdo) — Esse comando verifica o tamanho da mensagem enviada por solicitação ou resposta. A ação permitir ou redefinir pode ser aplicada a uma solicitação ou resposta que corresponda aos critérios de mapa de classe. A adição da ação de registro causa uma mensagem syslog:

`APPFW-4- HTTP_CONTENT_LENGTH`

Uso do comando:

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

Exemplos de casos de uso

Configure uma política http appfw para bloquear uma sessão http que transporta mais de 10 mil bytes de mensagem em uma solicitação ou resposta.

```
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
```

Status line inspection — O comando permite que o usuário especifique uma lista de expressões regulares para corresponder à linha de status de uma resposta. A ação permitir ou redefinir pode ser aplicada a uma solicitação ou resposta que corresponda aos critérios de mapa de classe. A adição da ação de registro causa uma mensagem syslog:

```
APPFW-6-HTTP_STLINE_REGEX_MATCHED
```

Uso do comando:

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

Exemplos de casos de uso

Configure um appfw http para registrar um alarme sempre que for feita uma tentativa de acessar uma página proibida. Uma página proibida geralmente contém um código de status 403 e a linha de status se parece com `HTTP/1.0 403 página proibida\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 inspection — Esse comando verifica se o tipo de conteúdo do cabeçalho da mensagem está na lista de tipos de conteúdo compatíveis. Também verifica se o tipo de conteúdo do cabeçalho corresponde ao conteúdo dos dados da mensagem ou da parte do corpo da entidade. Se a palavra mismatch estiver configurada, o comando verificará o tipo de conteúdo da mensagem de resposta em relação ao valor do campo aceito da mensagem de solicitação. A ação permitir ou redefinir pode ser aplicada a uma solicitação ou resposta que corresponda aos critérios de mapa de classe. A adição da ação de registro causa a mensagem de syslog apropriada:

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

  Uso do comando:

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

  Exemplos de casos de usoConfigure uma política http appfw para bloquear uma sessão http que transporta solicitações e respostas com um tipo de conteúdo desconhecido.

  ```
  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
  ```

Inspeção de mau uso de porta — Este comando é usado para evitar que a porta http (80) seja mal usada para outras aplicações, como IM, P2P, Tunelamento e assim por diante. A ação Permitir ou Redefinir pode ser aplicada a uma solicitação ou resposta que corresponda aos critérios de mapa de classe. A adição da ação de registro causa a mensagem de syslog apropriada:

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

Uso do comando:

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

Exemplos de casos de uso

Configure uma política http appfw para bloquear uma sessão http usada incorretamente para o aplicativo IM.

```
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 — Esse comando ativa a verificação de conformidade do protocolo estrito contra solicitações e respostas HTTP. A ação permitir ou redefinir pode ser aplicada a uma solicitação ou resposta que corresponda aos critérios de mapa de classe. A adição da ação de registro causa uma mensagem syslog:
  `APPFW-4- HTTP_PROTOCOL_VIOLATION`
  Uso do comando:
  `match req-resp protocol-violation`
  Exemplos de casos de usoConfigure uma política http appfw para bloquear solicitações ou respostas que violem o 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
  ```
- Inspeção de codificação de transferência — Este comando fornece a capacidade de permitir, negar ou monitorar solicitação/resposta cujo tipo de codificação de transferência corresponde ao tipo configurado. A ação permitir ou redefinir pode ser aplicada a uma solicitação ou resposta que corresponda aos critérios de mapa de classe. A adição da ação de registro causa uma mensagem syslog:
  `APPFW-6- HTTP_TRANSFER_ENCODING`
  Uso do comando:
  ```
  match {request|response|req-resp} header transfer-encoding
  {regex <parameter-map-name> |gzip|deflate|chunked|identity|all}
  ```
  Exemplos de casos de usoConfigure uma política http appfw para bloquear uma solicitação ou resposta que tenha a codificação de tipo compactado.
  ```
  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 — Esse comando verifica se uma resposta tem java applet e aplica a ação configurada durante a detecção do applet. A ação permitir ou redefinir pode ser aplicada a uma solicitação ou resposta que corresponda aos critérios de mapa de classe. A adição da ação de registro causa uma mensagem syslog:
  `APPFW-4- HTTP_JAVA_APPLET`
  Uso do comando:
  `match response body java-applet`
  Exemplos de casos de usoConfigure uma política http appfw para bloquear applets do Java.
  `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
```

Suporte ZFW para mensagens instantâneas e controle de aplicação peer-to-peer

O software Cisco IOS versão 12.4(9)T apresentou suporte ZFW para aplicações P2P e de IM.

O software Cisco IOS primeiro ofereceu suporte para controle de aplicação de IM no software Cisco IOS versão 12.4(4)T. A versão inicial do ZFW não foi compatível com a aplicação de IM na interface ZFW. Se o controle de aplicação de IM foi desejado, os usuários não conseguiram migrar para a interface de configuração do ZFW. O Cisco IOS Software Release 12.4(9)T introduz o suporte ZFW para Inspeção IM, que suporta o Yahoo! Messenger (YM), MSN Messenger (MSN) e AOL Instant Messenger (AIM). O Cisco IOS Software Release 12.4(9)T é a primeira versão do Cisco IOS Software que oferece suporte nativo do Cisco IOS Firewall para aplicativos de compartilhamento de arquivos P2P.

A inspeção de IM e P2P oferece políticas de Camada 4 e Camada 7 para tráfego de aplicações. Isso significa que o ZFW pode fornecer inspeção stateful básica para permitir ou negar o tráfego, bem como controle granular da camada 7 em atividades específicas nos vários protocolos, de modo que certas atividades de aplicativos sejam permitidas, enquanto outras são negadas.

Inspeção e controle de aplicação P2P

O SDM 2.2 introduziu o controle de aplicação P2P na seção de configuração do firewall. O SDM aplicou uma política de reconhecimento de aplicativo baseado em rede (NBAR) e QoS para detectar e vigiar a atividade de aplicativo P2P a uma taxa de linha de zero e bloquear todo o tráfego P2P. Isso levantou o problema de que os usuários da CLI, que esperavam suporte P2P na CLI do Cisco IOS Firewall, não conseguiram configurar o bloqueio P2P na CLI, a menos que estivessem cientes da configuração necessária de NBAR/QoS. O Cisco IOS Software Release 12.4(9)T introduz o controle P2P nativo na CLI do ZFW, para aproveitar o NBAR para detectar a atividade do aplicativo P2P. Esta versão do software aceita vários protocolos de aplicação P2P:

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

As aplicações P2P são particularmente difíceis de detectar, como resultado de um comportamento de "salto de porta" e outros truques para evitar a detecção, bem como os problemas introduzidos por alterações e atualizações frequentes em aplicações P2P que modificam os comportamentos dos protocolos. O ZFW combina a inspeção nativa de firewall stateful com os recursos de reconhecimento de tráfego do NBAR para oferecer controle de aplicação P2P na interface de configuração CPL do ZFW. O NBAR oferece dois benefícios excelentes:

- Reconhecimento de aplicações de acordo com heurística opcional para reconhecê-las, apesar de um comportamento complexo e de difícil detecção

- Infraestrutura extensível que oferece um mecanismo de atualização para acompanhar as atualizações e modificações do protocolo

Configurar Inspeção P2P

Como mencionado anteriormente, a inspeção e o controle P2P oferecem a inspeção stateful de Camada 4 e o controle de aplicação da Camada 7. A inspeção da camada 4 é configurada de forma semelhante a outros serviços de aplicativos, se a inspeção das portas de serviço de aplicativos nativos for adequada:

```
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]
```

Observe a opção de assinatura adicional no protocolo de correspondência [service-name]. Quando a opção de assinatura é adicionada ao final da instrução do protocolo de correspondência, a heurística de NBAR é aplicada ao tráfego para procurar por indicadores no tráfego que indiquem atividade específica do aplicativo P2P. Isso inclui o salto da porta e outras alterações no comportamento da aplicação para evitar a detecção de tráfego. Esse nível de inspeção de tráfego tem o preço de aumento da utilização da CPU e do recurso de taxa de transferência de rede reduzida. Se a opção de assinatura não for aplicada, a análise heurística baseada em NBAR não será aplicada para detectar o comportamento de salto de porta e a utilização da CPU não sofrerá impacto na mesma extensão.

A inspeção de serviço nativo tem a desvantagem de impossibilitar o controle sobre aplicações P2P, caso os "saltos" da aplicação não tenha uma porta de origem e destino, ou se a aplicação for atualizada para iniciar a ação em um número de porta não reconhecido:

Aplicativo	Portas nativas (conforme reconhecidas pela lista de PAM 12.4(15)T)
bittorrent	TCP 6881-6889
eDonkey	TCP 4662
fasttrack	TCP 1214
gnutella	TCP 6346-6349 TCP 6355,5634 UDP 6346-6348
kazaa2	Dependente do PAM
winmx	TCP 6699

Se desejar permitir (inspecionar) o tráfego P2P, você poderá precisar fornecer configuração adicional. Alguns aplicativos podem usar várias redes P2P ou implementar comportamentos específicos que você pode precisar acomodar na configuração do firewall para permitir que o aplicativo funcione:

- Os clientes BitTorrent geralmente se comunicam com "rastreadores" (servidores de diretório pares) através de http que são executados em alguma porta não padrão. Geralmente é o TCP 6969, mas você pode precisar verificar a porta do rastreador específica do torrent. Se você quiser permitir o BitTorrent, o melhor método para acomodar a porta adicional é configurar o HTTP como um dos protocolos de correspondência e adicionar o TCP 6969 ao HTTP com o comando ip port-map:
  `ip port-map http port tcp 6969`

Você precisa definir http e bittorrent como os critérios de correspondência aplicados no mapa de classes.

- O eDonkey parece iniciar as conexões que são detectadas como eDonkey e Gnutella.
- A inspeção KaZaA é totalmente dependente da detecção de assinatura NBAR.

A Inspeção da Camada 7 (Aplicação) aumenta a Inspeção da Camada 4 com a capacidade de reconhecer e aplicar ações específicas do serviço, como bloquear ou permitir seletivamente recursos de pesquisa de arquivos, transferência de arquivos e bate-papo de texto. Os recursos específicos de serviço variam de acordo com o serviço.

A inspeção de aplicação P2P é semelhante à inspeção de aplicação HTTP:

```
!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
```

A inspeção de aplicações P2P oferece recursos específicos da aplicação para um subconjunto de aplicações compatíveis com a inspeção da Camada 4:

- eDonkey
- fasttrack
- gnutella
- kazaa2

Cada um desses aplicativos oferece opções variáveis de critérios de correspondência específicos do aplicativo:

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
```

fasttrack

```
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
```

Novas definições de protocolo P2P ou atualizações para protocolos P2P atuais podem ser carregadas com a funcionalidade de atualização dinâmica de pdlm do NBAR. Este é o comando de configuração para carregar o novo PDLM:

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

O novo protocolo está disponível em comandos match protocol para inspeção de tipo de classe. Se o novo protocolo P2P tiver serviços (subprotocolos), os novos tipos de class-map inspecionados da Camada 7, bem como os critérios de correspondência da Camada 7, ficarão disponíveis.

Controle e inspeção de aplicação de IM

O software Cisco IOS versão 12.4(4)T introduziu a inspeção e o controle de aplicação de IM. O suporte a IM não foi introduzido com o ZFW na versão 12.4(6)T, portanto, os usuários não conseguiram aplicar o controle de IM e ZFW na mesma política de firewall, pois os recursos de firewall e ZFW herdados não podem coexistir em uma determinada interface.

O software Cisco IOS versão 12.4(9)T é compatível com inspeção stateful e controle de aplicação para esses serviços de IM:

- (por exemplo: Instant Messenger)
- MSN Messenger
- Yahoo! Messenger

A inspeção de IM varia um pouco da maioria dos serviços, já que a inspeção de IM controla o acesso a um grupo específico de hosts para cada serviço fornecido. Os serviços de IM geralmente dependem de um grupo relativamente permanente de servidores de diretório, com os quais os clientes devem ser capazes de entrar em contato para acessar o serviço de IM. As aplicações de IM costumam ser muito difíceis de controlar, de um ponto de vista de protocolo ou serviço. A maneira mais eficaz de controlar essas aplicações é limitar o acesso aos servidores de IM fixos.

Configurar Inspeção de IM

A inspeção e o controle de mensagens instantâneas oferecem inspeção stateful de camada 4

e controle de aplicação da camada 7.

A inspeção da Camada 4 é configurada da mesma forma que outros serviços de aplicações:

```
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
```

As aplicações de IM podem entrar em contato com seus servidores em várias portas para manter a funcionalidade. Para permitir um determinado serviço de IM com a ação de inspeção, você não pode precisar de uma lista de servidores para definir o acesso permitido aos servidores do serviço de IM. No entanto, quando você configura um mapa de classe que especifica um determinado serviço de IM, como o AOL Instant Messenger, e aplica a ação de soltar no mapa de política associado pode fazer com que o cliente de IM tente localizar uma porta diferente onde a conectividade é permitida para a Internet. Se você não quiser permitir a conectividade com um determinado serviço ou se quiser restringir a capacidade de serviço de IM para o bate-papo por texto, você deve definir uma lista de servidores para que o ZFW possa identificar o tráfego associado à aplicação de IM:

```
!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
```

Por exemplo, a lista de servidor de IM do Yahoo é definida da seguinte forma:

```
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
```

Você precisa aplicar a lista de servidores à definição de protocolo:

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

Você deve configurar os comandos ip domain lookup e ip name-server ip.ad.re.ss em ordem para habilitar a resolução do nome.

Os nomes dos servidores de IM são razoavelmente dinâmicos. Você precisa verificar periodicamente se suas listas de servidores de IM configuradas estão completas e corretas.

A Inspeção da Camada 7 (Aplicação) aumenta a Inspeção da Camada 4 com a capacidade de reconhecer e aplicar ações específicas do serviço, como bloquear ou permitir seletivamente recursos de bate-papo de texto e negar outros recursos do serviço.

A inspeção do aplicações de IM atualmente oferece a capacidade de diferenciar a atividade de bate-papo por texto e todos os outros serviços de aplicações. Para restringir a atividade de IM para o bate-papo por texto, configure uma política de Camada 7:

```
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]
```

Aplique a política da Camada 7 ao Yahoo! Política do Messenger configurada anteriormente:

```
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
```

Filtros de URL

O ZFW oferece recursos de filtragem de URL para limitar o acesso ao conteúdo da Web ao especificado por uma lista branca ou negra definida no roteador ou encaminhando nomes de domínio para um servidor de filtragem de URL para verificar o acesso a domínios específicos. A filtragem de URL ZFW no software Cisco IOS versões 12.4(6)T a 12.4(15)T é aplicada como uma ação de política adicional, semelhante à inspeção da aplicação.

Para a filtragem de URL baseada em servidor, você deve definir um mapa de parâmetros que descreva a configuração do servidor urlfilter:

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

Se as listas estáticas de permissão ou bloqueio forem preferidas, você poderá definir uma lista de domínios ou subdomínios que sejam especificamente permitidos ou negados, enquanto a ação inversa é aplicada ao tráfego que não corresponde à lista:

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

Se uma lista negra de URL for definida com opções de negação nas definições de domínio exclusivo, todos os outros domínios serão permitidos. Se forem definidas definições de "permissão", todos os domínios permitidos deverão ser explicitamente especificados, de forma semelhante à função das listas de controle de acesso IP.

Configure um mapa de classe que corresponda ao tráfego HTTP:

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

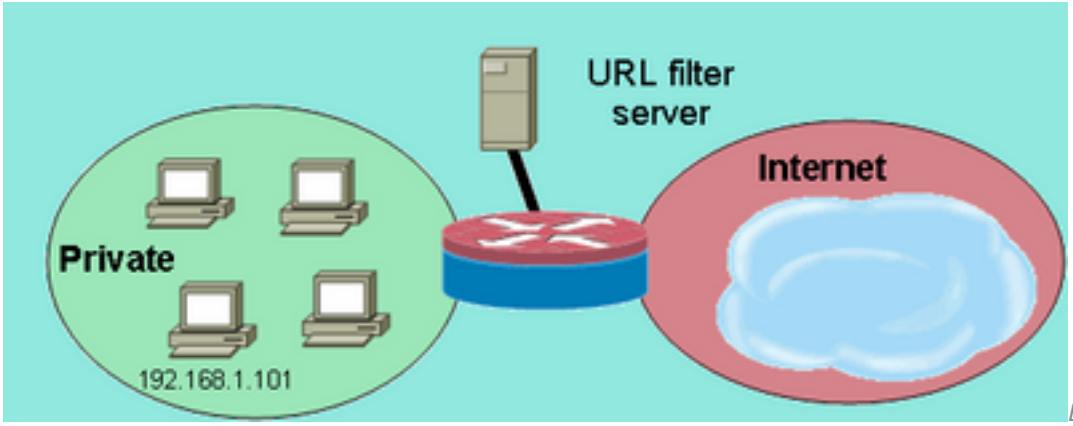
Defina um policy-map que associa o class-map às açõesinspect e urlfilter:

```
policy-map type inspect http-filter-pmap
 class type inspect http-cmap
  inspect
  urlfilter websense-parmap
```

Isso configura o requisito mínimo para se comunicar com um servidor de filtragem de URL. Várias opções estão disponíveis para definir o comportamento adicional de filtragem de URL.

Algumas implantações de rede desejam aplicar a filtragem de URL para alguns hosts ou sub-redes e ignorar a filtragem de URL para outros hosts. Por exemplo, na Figura 9, todos os hosts na zona privada devem ter o tráfego HTTP verificado por um servidor de filtro de URL, exceto pelo host específico 192.168.1.101.

Figura 10: Exemplo de topologia de filtragem de URL



Exemplo de topologia de filtragem de URL

Isso pode ser realizado se você definir dois mapas de mapa de classe diferentes:

- Um mapa de classe que corresponde apenas ao tráfego HTTP para o grupo maior de hosts, que recebem filtragem de URL.
- Um mapa de classe para o grupo menor de hosts, que não recebe filtragem de URL. O segundo mapa de classe corresponde ao tráfego HTTP, bem como uma lista de hosts que estão isentos da política de filtragem de URL.

Ambos os mapas de classe são configurados em um mapa de política, mas somente um recebe a ação urlfilter:

```
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
```

Controle o acesso ao roteador

A maioria dos engenheiros de segurança de rede não se sente confortável se expõem as interfaces de gerenciamento do roteador (por exemplo, SSH, Telnet, HTTP, HTTPS, SNMP e assim por diante) à Internet pública e, em determinadas circunstâncias, o controle também é necessário para o acesso da LAN ao roteador. O software Cisco IOS oferece uma série de opções para limitar o acesso às várias interfaces, que inclui a família de recursos de proteção da base de rede (NFP), vários mecanismos de controle de acesso para interfaces de gerenciamento e a zona automática do ZFW. Você deve rever outros recursos, como controle de acesso VTY, proteção do plano de gerenciamento e controle de acesso SNMP para determinar qual combinação de recursos de controle do roteador funciona melhor para seu aplicativo específico.

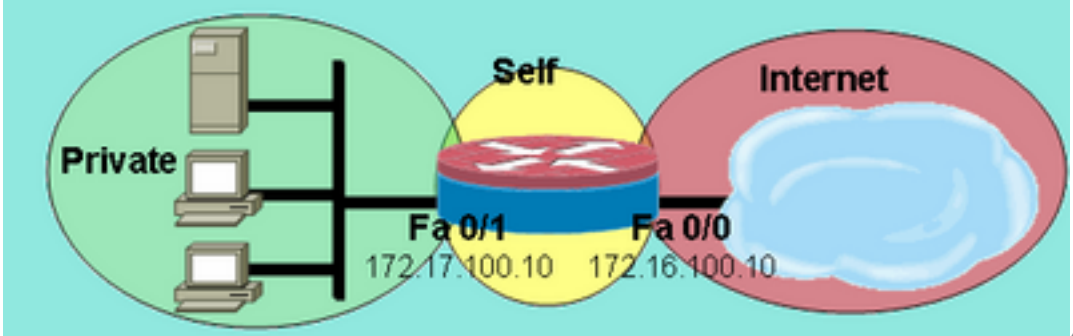
Geralmente, a família de recursos NFP é mais adequada para o controle do tráfego destinado ao próprio roteador. Consulte Visão Geral da Segurança do Plano de Controle no Cisco IOS Software para obter informações que descrevem a proteção do roteador com os recursos NFP.

Se decidir aplicar ZFW para controlar o tráfego de e para os endereços IP no próprio roteador, você deverá entender que a política e os recursos padrão do firewall diferem dos disponíveis para o tráfego de trânsito. O tráfego de trânsito é definido como o tráfego de rede cujos endereços IP origem e destino não correspondem a nenhum endereço IP aplicado a qualquer uma das interfaces do roteador, e o tráfego não faz com que o roteador envie, por exemplo, mensagens de controle de rede como expiração de TTL ICMP ou mensagens de rede/host inalcançável.

O ZFW aplica uma política deny-all padrão ao tráfego que se move entre as zonas, exceto, como mencionado nas regras gerais, o tráfego em qualquer zona que flui diretamente para os endereços das interfaces do roteador é permitido implicitamente. Isso garante que a conectividade com as interfaces de gerenciamento do roteador seja mantida quando uma configuração de firewall da zona for aplicada ao roteador. Se a mesma política de negar tudo afetasse a conectividade diretamente ao roteador, uma configuração completa da política de gerenciamento teria que ser aplicada antes que as zonas fossem configuradas no roteador. Isso provavelmente interromperia a conectividade de gerenciamento, se a política fosse implementada de forma adequada ou aplicada na ordem errada.

Quando uma interface é configurada para ser um membro da zona, os hosts conectados à interface são incluídos na zona. No entanto, o tráfego que flui de e para os endereços IP das interfaces do roteador não é controlado pelas políticas de zona (com exceção das circunstâncias descritas na observação na Figura 10). Em vez disso, todas as interfaces IP no roteador são automaticamente parte da zona automática quando o ZFW é configurado. Para controlar o tráfego IP que se move para as interfaces do roteador a partir de várias zonas em um roteador, as políticas devem ser aplicadas para bloquear ou permitir/inspecionar o tráfego entre a zona e a autozona do roteador e vice-versa (consulte a Figura 11).

Figura 11: Aplicar política entre zonas de rede e autozona do roteador



Aplicar política entre zonas de rede e autozona do roteador

Embora o roteador ofereça uma política de permissão padrão entre todas as zonas e a zona automática, se uma política for configurada de qualquer zona para a zona automática e nenhuma política for configurada de zonas autoconectadas à interface configurável pelo usuário do roteador, todo o tráfego originado pelo roteador encontra a política de zona conectada para zona automática em seu retorno ao roteador e é bloqueado. Assim, o tráfego originado no roteador deve ser inspecionado para permitir seu retorno à autozona.

> **Note**: O software Cisco IOS sempre usa o endereço IP associado a um host de destino "mais próximo" de interface para tráfego como syslog, TFTP, Telnet e outros serviços de plano de controle e sujeita esse tráfego à política de firewall autozona. No entanto, se um serviço definir uma interface específica como a interface de origem com comandos que incluem, mas não se limitam a, logging source-interface [type number] , ip tftp source-interface [type number] e ip telnet source-interface [type number] , o tráfego estará sujeito à autozona.

> **Nota**:Alguns serviços (particularmente os serviços de voz sobre IP dos roteadores) usam interfaces efêmeras ou não configuráveis que não podem ser atribuídas a zonas de segurança. Esses serviços não poderão funcionar corretamente se o tráfego não puder ser associado a uma zona de segurança configurada.

Limitações de política de autozona

A política de zona tem funcionalidade limitada, em comparação às políticas disponíveis para transit-traffic zone-pairs:

- Como foi o caso na inspeção clássica stateful, o tráfego gerado pelo roteador está limitado a TCP, UDP, ICMP e inspeção de protocolo complexo para H.323.
- A inspeção de aplicações não está disponível para políticas de autozona.
- A limitação de sessão e de taxa não pode ser configurada em políticas de autozona.

Configuração de política

Na maioria das vezes, essas são políticas de acesso desejáveis para os serviços de gerenciamento de roteador:

- Negar toda a conectividade de Telnet, pois o protocolo de texto simples de Telnet expõe facilmente as credenciais do usuário e outras informações confidenciais.
- Permitir conexões SSH de qualquer usuário em qualquer zona. O SSH criptografa as credenciais do usuário e os dados da sessão, o que fornece proteção contra usuários mal-intencionados que empregam ferramentas de captura de pacotes para espionar a atividade do usuário e comprometer as credenciais do usuário ou informações confidenciais, como a configuração do roteador. O SSH Versão 2 fornece proteção mais forte e aborda vulnerabilidades específicas inerentes ao SSH Versão 1.
- Permita a conectividade HTTP para o roteador a partir de zonas privadas se a zona privada for confiável. Caso contrário, se a zona privada abrigar o potencial de usuários mal-intencionados comprometerem informações, o HTTP não emprega criptografia para proteger o tráfego de gerenciamento e pode revelar informações confidenciais, como credenciais ou configuração do usuário.

- Permitir conectividade HTTPS de qualquer zona. Semelhante ao SSH, o HTTPS criptografa os dados da sessão e as credenciais do usuário.
- Restrinja o acesso de SNMP a um host ou a uma sub-rede específica. O SNMP pode ser usado para modificar a configuração do roteador e revelar as informações de configuração. O SNMP deve ser configurado com controle de acesso nas várias comunidades.
- Bloqueie solicitações ICMP da Internet pública para o endereço da zona privada (isso pressupõe que o endereço da zona privada seja roteável). Um ou mais endereços públicos podem ser expostos para tráfego ICMP para a solução de problemas de rede, se necessário. Vários ataques de ICMP podem ser usados para sobrecarregar os recursos do roteador ou fazer o reconhecimento da topologia e a arquitetura de rede.

Um roteador pode aplicar esse tipo de política com a adição de dois zone-pairs para cada zona que deve ser controlada. Cada par de zonas para tráfego de entrada ou saída da autozona do roteador deve ser correspondido pela respectiva política na direção oposta, a menos que o tráfego não seja originado na direção oposta. Um policy-map cada para zone-pairs de entrada e saída pode ser aplicado, descrevendo todo o tráfego, ou os policy-maps específicos por zone-pair podem ser aplicados. A configuração de pares de zonas específicos por mapa de políticas fornece granularidade para visualizar a atividade que corresponde a cada mapa de políticas.

Um exemplo de rede com uma estação de gerenciamento SNMP em 172.17.100.11 e um servidor TFTP em 172.17.100.17, esta saída fornece um exemplo de toda a política de acesso da interface de gerenciamento:

```
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
```

Infelizmente, a política de autozona não oferece a capacidade de inspecionar transferências TFTP. Assim, o firewall deve transmitir todo o tráfego de entrada e saída do servidor TFTP, se o TFTP precisar passar pelo firewall.

Se o roteador terminar conexões VPN IPSec, você também deverá definir uma política para passar IPSec ESP, IPSec AH, ISAKMP e NAT-T IPSec (UDP 4500). Isso depende do que é necessário com base nos serviços que você usa. Essa próxima política pode ser aplicada além da política acima. Observe a alteração nos mapas de política onde um mapa de classe para tráfego VPN foi inserido com uma ação de passagem. Geralmente, o tráfego criptografado é confiável, a não ser que a política de segurança declare que você deve permitir o tráfego criptografado de entrada e saída de endpoints especificados.

```
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
```

Serviços de firewall de acordo com a zona e aplicação de área remota

Consulte Release Note para Cisco Wide Area Application Services (Versão de Software 4.0.13) - Novos Recursos para a Versão de Software 4.0.13 para obter uma nota de aplicativo que fornece exemplos de configuração e orientação de uso

Monitore o firewall de política baseado em zona com os comandos show e debug

O ZFW apresenta novos comandos para exibir a configuração da política e monitorar a atividade do firewall.

Exibe a descrição da zona e as interfaces contidas em uma zona especificada:

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

Quando o nome da zona não é incluído, o comando exibe as informações de todas as zonas configuradas.

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

Exibe a zona de origem, a zona de destino e a política conectada ao zone-pair:

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

Quando nenhuma origem ou destino é especificado, todos os zone-pairs com origem, destino e a política associada são exibidos. Quando apenas a zona de origem/destino é mencionada, todos os zone-pairs que contêm essa zona como origem/destino são exibidos.

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

Exibe um mapa de políticas especificado:

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

Quando o nome de um mapa de políticas não é especificado, ele exibe todos os mapas de políticas do tipo inspect (juntamente com os mapas de políticas da camada 7 que contêm um subtipo).

```
Router#show policy-map type inspect p1
```

```
 Policy Map type inspect p1
   Class c1
    Inspect
```

Exibe as estatísticas de mapa de política de tipo de inspeção de tempo de execução atualmente em um par de zonas especificado.

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

Quando no zone-pair name é mencionado, policy-maps em todos zone-pairs são exibidos.

A opção sessions exibe as sessões de inspeção criadas pela aplicação policy-map no zone-pair especificado.

```
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
```

A palavra-chave urlfilter exibe as estatísticas relacionadas a urlfilter que pertencem ao policy-map especificados (ou policy-maps em todos os destinos quando o zone-pair name é especificado):

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

Quando a palavra-chave cache é especificada com urlfilter, ela exibe o cache urlfilter (dos endereços IP).

Resumo do comando show policy-map para policy-maps de inspeção:

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

Ajustar a proteção de negação de serviço do firewall de política

baseada em zona

O ZFW oferece proteção de DoS para alertar os engenheiros de rede que façam alterações drásticas na atividade da rede e reduzam a atividade indesejada para minimizar o impacto das alterações na atividade da rede. O ZFW mantém um contador separado para cada class-map de policy-map. Assim, se um mapa de classe é usado para dois mapas de política de pares de zonas diferentes, dois conjuntos diferentes de contadores de proteção DoS são aplicados.

O ZFW fornece mitigação de ataques de DoS como um padrão nas versões de software Cisco IOS antes de 12.4(11)T. O comportamento de proteção de DoS padrão mudou com o software Cisco IOS versão 12.4(11)T.

Consulte Definição de estratégias para proteção contra ataques de negação de serviço de SYN de TCPpara obter mais informações sobre ataques de DoS de SYN de TCP.

Apêndices

Apêndice A: Configuração básica

```
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
```

Apêndice B: Configuração final (completa)

```
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
```

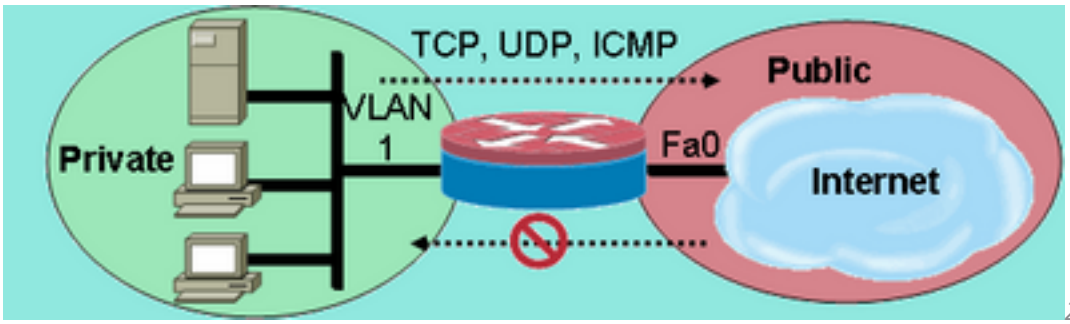
```
 class type inspect dns-http-acl-class
  inspect
 class type inspect smtp-acl-class
  inspect
policy-map type inspect servers-clients-policy
 class type inspect Xwindows-class
  inspect
policy-map type inspect private-internet-policy
  class type inspect internet-traffic-class
   inspect
  class 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
```

Apêndice C: Configuração básica de firewall de política de acordo com a zona para duas zonas

Este exemplo fornece uma configuração simples como base para testar recursos para aprimoramentos no Cisco IOS Software ZFW. Essa configuração é uma configuração de modelo para duas zonas, conforme configurado em um roteador 1811. A zona privada é aplicada às portas fixas do switch do roteador, portanto todos os hosts nas portas do switch são conectados à VLAN 1. A zona pública é aplicada à FastEthernet 0 (consulte a Figura 12).

Figura 12: Zona pública aplicada em FastEthernet 0



Zona pública aplicada em FastEthernet 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
```

Informações Relacionadas

- Suporte Técnico e Documentação - Cisco Systems

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.