Projeto do Firewall da política e guia Zona-baseados do aplicativo

Índice

Introdução

O Software Release 12.4(6)T de Cisco IOS® introduzido Zona-baseou o Firewall da política (ZFW), um modelo novo da configuração para o Cisco IOS Firewall Feature Set. Este modelo novo da configuração oferece políticas intuitivas para o Roteadores da interface múltipla, a

granularidade aumentada do aplicativo da política de firewall, e um padrão negar-toda política que proibe o tráfego entre zonas de Segurança do Firewall até que uma política explícita esteja aplicada para permitir o tráfego desejável.

Quase todos os recursos de firewall do IOS Cisco clássico executados antes que o Cisco IOS Software Release 12.4(6)T estiver apoiado na relação zona-baseada nova da inspeção da política:

- Inspeção de pacote de informação do stateful
- Cisco IOS Firewall VRF-ciente
- Filtragem URL
- Mitigação da recusa de serviço (DoS)

Cisco IOS Software Release 12.4(9)T apoio adicionado inspeção de aplicativo ZFW para por classe limites da sessão/conexão e da taxa de transferência, assim como e controle:

- HTTP
- O protocolo Post Office Protocol (POP3), o protocolo de acesso do correio de Internet (IMAP), protocolo simple mail transfer/aumentou o protocolo simple mail transfer (SMTP/ESMTP)
- Chamada de procedimento remoto de Sun (RPC)
- Aplicativos das mensagens instantâneas (IM):Mensageiro de MicrosoftYahoo! MensageiroAOL Instant Messenger
- Compartilhamento de arquivo (P2P) peer-to-peer:BittorrentKaZaAGnutellaeDonkey

Estatísticas adicionadas Cisco IOS Software Release 12.4(11)T para o ajustamento mais fácil da proteção de DOS.

Alguns recursos de firewall e capacidades clássicos do Cisco IOS não são apoiados ainda em um ZFW no Cisco IOS Software Release 12.4(15)T:

- Proxy de autenticação
- Failover do firewall stateful
- Firewall unificado MIB
- Inspeção stateful do IPv6
- Apoio fora de serviço TCP

ZFW melhora geralmente o desempenho do Cisco IOS para a maioria de atividades da inspeção do Firewall.

Nem o Cisco IOS ZFW ou o Firewall clássico incluem o apoio da inspeção stateful para o tráfego multicast.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

Convenções

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

Vista geral Zona-baseada da política

A inspeção stateful clássica do Firewall do Cisco IOS (conhecida anteriormente como o Context-Based Access Control, ou o CBAC) empregou um modelo relação-baseado da configuração, em que uma política da inspeção stateful foi aplicada a uma relação. Todo o tráfego que passa através dessa relação recebeu a mesma política da inspeção. Este modelo da configuração limitou a granularidade das políticas de firewall e causou a confusão do aplicativo apropriado das políticas de firewall, particularmente nas encenações quando as políticas de firewall devem ser aplicadas entre interfaces múltiplas.

O Firewall Zona-baseado da política (igualmente conhecido como o Firewall da Zona-política, ou o ZFW) muda a configuração de firewall do modelo relação-baseado mais velho a um modelo zona-baseado mais flexível, mais de fácil compreensão. As relações são atribuídas às zonas, e a política da inspeção é aplicada para traficar mover-se entre as zonas. as políticas da Inter-zona oferecem a flexibilidade e a granularidade consideráveis, assim que as políticas diferentes da inspeção podem ser aplicadas aos grupos do host múltiplo conectados à relação do mesmo roteador.

As políticas de firewall são configuradas com a língua da política de Cisco® (COMPLETA), que emprega uma estrutura hierárquica para definir a inspeção para protocolos de rede e os grupos de anfitriões a que a inspeção será aplicada.

Modelo Zona-baseado da configuração das normas

ZFW muda completamente a maneira que você configura uma inspeção do Cisco IOS Firewall, em relação ao Firewall do clássico do Cisco IOS.

A primeira alteração principal à configuração de firewall é a introdução de configuração zona-baseada. O Cisco IOS Firewall é a primeira característica da defesa da ameaça do Cisco IOS Software para executar um modelo da configuração da zona. Os outros recursos puderam adotar o modelo da zona ao longo do tempo. A inspeção stateful clássica do Firewall do Cisco IOS (ou o CBAC) relação-basearam o modelo da configuração que emprega o grupo do **comando ip inspect** são mantidos por um período de tempo. Contudo, poucos, eventualmente, novos recursos são configuráveis com o comando line interface(cli) clássico. ZFW não usa a inspeção stateful ou comandos CBAC. Os dois modelos da configuração podem ser usados simultaneamente no Roteadores, mas não ser combinados em relações. Uma relação não pode ser configurada como um membro da zona de Segurança assim como sendo configurado para o **IP inspecione** simultaneamente.

As zonas estabelecem as beiras da Segurança de sua rede. Uma zona define um limite onde o tráfego seja sujeitado às limitações da política como ele se cruze a uma outra região de sua rede. A política padrão de ZFW entre zonas é nega tudo. Se nenhuma política é configurada explicitamente, todo o tráfego que se move entre zonas está obstruído. Esta é uma partida significativa do modelo da inspeção stateful onde o tráfego foi permitido implicitamente até obstruído explicitamente com um Access Control List (ACL).

A segunda alteração principal é a introdução de uma língua nova da política da configuração conhecida como COMPLETO Usuários que o familiar com a Qualidade de Serviço modular do Cisco IOS Software (QoS) CLI (MQC) pôde reconhecer que o formato é similar ao uso de QoS de mapas da classe especificar que tráfego será afetado pela ação aplicada em um mapa de política.

Regras para aplicar o Firewall Zona-baseado da política

A sociedade de relações de rede do roteador nas zonas é sujeita a diversas regras que governam o comportamento da relação, como é o tráfego que se move entre interfaces membro da zona:

- Uma zona deve ser configurada antes que as relações possam ser atribuídas à zona.
- Uma relação pode ser atribuída a somente uma zona de Segurança.
- Todo o tráfego a e de uma dada interface é obstruído implicitamente quando a relação é atribuída a uma zona, a não ser que tráfego a e de outras relações na mesma zona, e tráfego a alguma relação no roteador.
- O tráfego é permitido implicitamente fluir à revelia entre as relações que são membros da mesma zona.
- A fim permitir o tráfego a e de uma interface membro da zona, uma política permitindo ou inspecionando o tráfego deve ser configurada entre essa zona e toda a outra zona.
- A zona do auto é a única exceção ao padrão nega toda a política. Todo o tráfego a toda a interface do roteador é permitido até que o tráfego esteja negado explicitamente.
- O tráfego não pode fluir entre uma interface membro da zona e nenhuma relação que não for um membro da zona. A passagem, inspeciona, e as ações de queda podem somente ser aplicadas entre duas zonas.
- Relações que não foram atribuídas a uma função da zona como portas de roteador clássicas e puderam ainda usar a configuração clássica do stateful inspection/CBAC.
- Se se exige que uma relação na caixa não ser parte do Zoneamento/política de firewall. Pôde ainda ser necessário pôr que relação em uma zona e configura uma passagem toda a política (meio uma política do manequim) entre essa zona e toda a outra zona a que o fluxo de tráfego for desejado.
- Da precedência segue que, se o tráfego é fluir entre todas as relações em um roteador, todas as relações devem ser parte do modelo do Zoneamento (cada relação deve ser um membro de uma zona ou de outra).
- A única exceção à precedência nega à revelia a aproximação é o tráfego a e do roteador, que será permitido à revelia. Uma política explícita pode ser configurada para restringir tal tráfego.

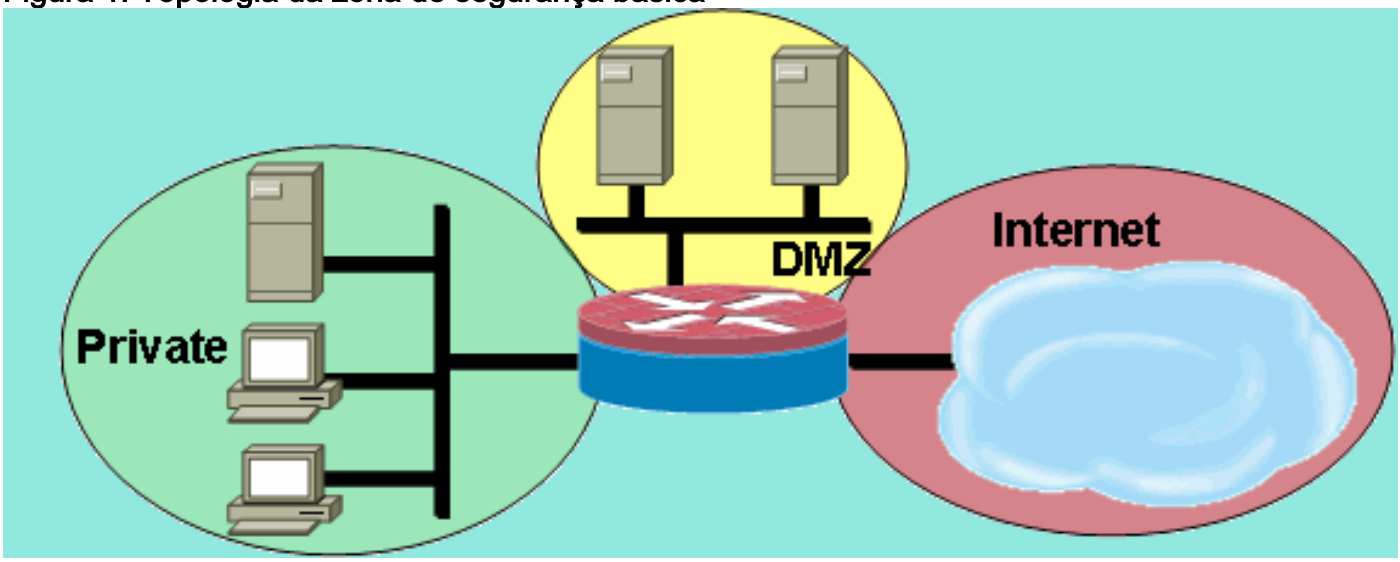
Projetando a Segurança Zona-baseada da rede de política

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

- Uma relação conectada aos Internet públicas
- Uma relação conectada a uma LAN privada que não deva ser acessível dos Internet públicas
- Uma relação conectada a uma zona desmilitarizada do serviço de Internet (DMZ), onde um server do servidor de Web, do Domain Name System (DNS), e o server do email devem ser acessíveis aos Internet públicas

Cada relação nesta rede será atribuída a sua própria zona, embora você possa querer permitir acesso variado dos Internet públicas aos anfitriões específicos no DMZ e das políticas variadas do uso do aplicativo para anfitriões no LAN protegido. (Veja figura 1.)

Figura 1: Topologia da zona de segurança básica



Neste exemplo, cada zona guarda somente uma relação. Se uma interface adicional é adicionada à zona privada, os anfitriões conectados à relação nova na zona podem passar o tráfego a todos os anfitriões na interface existente na mesma zona. Adicionalmente, o tráfego dos anfitriões aos anfitriões em outras zonas é afetado similarmente por políticas existentes.

Tipicamente, a rede de exemplo terá três políticas principais:

- Conectividade privada da zona ao Internet
- Conectividade privada da zona aos anfitriões DMZ
- Conectividade da zona do Internet aos anfitriões DMZ

Porque o DMZ é exposto aos Internet públicas, os anfitriões DMZ puderam ser sujeitados a atividade indesejada dos indivíduos maliciosos que puderam suceder em comprometer uns ou vários anfitriões DMZ. Se nenhuma política de acesso é fornecida para que os anfitriões DMZ alcancem anfitriões privados dos anfitriões da zona ou da zona do Internet, a seguir os indivíduos que comprometeram os anfitriões DMZ não podem usar os anfitriões DMZ para realizar o futuro ataque contra privado ou host de Internet. ZFW impõe uma postura de segurança proibitiva do padrão. Consequentemente, a menos que os anfitriões DMZ forem especificamente acesso fornecido a outras redes, outras redes são protegidas contra todas as conexões dos anfitriões DMZ. Similarmente, nenhum acesso é fornecido para que os host de Internet alcancem os anfitriões privados da zona, assim que os anfitriões privados da zona são seguros de acesso indesejável por host de Internet.

Usando o IPSec VPN com o Firewall Zona-baseado da política

As melhorias recentes ao IPSec VPN simplificam a configuração da política de firewall para a conectividade de VPN. A interface de túnel virtual do IPsec (VTI) e GRE+IPSec permitem o confinamento da site para site e das conexões de cliente VPN a uma zona de Segurança específica colocando as interfaces de túnel em uma zona de Segurança especificada. As conexões podem ser isoladas em um VPN DMZ se a Conectividade deve ser limitada por uma política específica. Ou, se a conectividade de VPN é confiada implicitamente, a conectividade de VPN pode ser colocada na mesma zona de Segurança que a rede interna confiada.

Se um IPsec NON-VTI é aplicado, a política de firewall da conectividade de VPN exige o rigoroso escrutínio manter a Segurança. A política da zona deve especificamente permitir o acesso por um endereço IP de Um ou Mais Servidores Cisco ICM NT para os anfitriões dos locais remotos ou os clientes VPN se fixe anfitriões estão em uma zona diferente do que a conexão criptografada do cliente VPN ao roteador. Se a política de acesso não é configurada corretamente, os anfitriões que devem ser protegidos podem terminar exposto acima aos anfitriões indesejáveis, potencialmente hostis. Refira a utilização do VPN com o Firewall Zona-baseado da política para uma discussão mais adicional do conceito e da configuração.

Configuração (COMPLETA) da língua da política de Cisco

Este procedimento pode ser usado para configurar um ZFW. A sequência das etapas não é importante, mas alguns eventos devem ser terminados em ordem. Por exemplo, você deve configurar um mapa de classe antes que você atribua um mapa de classe a um mapa de política. Similarmente, você não pode atribuir um mapa de política a um zona-par até que você configure a política. Se você tenta configurar uma seção que confie em uma outra parcela da configuração que você não configurou, o roteador responde com um Mensagem de Erro.

1. Defina zonas.
2. Defina zona-pares.
3. Defina os mapas de classe que descrevem o tráfego que deve ter a política aplicada como ele cruza um zona-par.
4. Defina política-mapas para aplicar a ação ao tráfego dos seus mapas de classe.
5. Aplique política-mapas aos zona-pares.
6. Atribua relações às zonas.

Configurando mapas de classe Zona-baseados do Firewall da política

Os mapas de classe definem o tráfego que o Firewall seleciona para o aplicativo da política. Mergulhe 4 mapas de classe classificam o tráfego baseado nestes critérios alistados aqui. Estes critérios são especificados usando o **comando match em um** mapa de classe:

- Acesso-grupo — Um padrão, um prolongado, ou ACL nomeado podem filtrar tráfego baseado no endereço IP de origem e de destino e na porta de origem e de destino.
- Protocolo — Os protocolos da camada 4 (TCP, UDP, e ICMP) e serviços de aplicativo tais como o HTTP, o S TP, o DNS, etc. Todo o serviço conhecido ou definido pelo utilizador conhecido ao mapeamento da porta de aplicativo pode ser especificado.
- Mapa de classe — Um mapa de classe subordinado que fornece critérios de verificação de repetição de dados adicionais pode ser aninhado dentro de um outro mapa de classe.
- Não — *Não o* critério especifica que o mapa de classe de todo o tráfego que não combinar um serviço especificado (protocolo), de acesso-grupo ou de subordinado estará selecionado para o mapa de classe.

Combinando critérios do “fósforo”: “Compatível com qualquer” contra “compatível com todos”

Os mapas de classe podem aplicar os operadores compatíveis com qualquer ou compatíveis com todos para determinar como aplicar os critérios de verificação de repetição de dados. Se compatível com qualquer é especificado, tráfego deve encontrar somente um dos critérios de verificação de repetição de dados no mapa de classe. Se compatível com todos é especificado,

tráfego deve combinar os critérios de todos os classe-mapas a fim pertencer a essa classe particular.

Os critérios de verificação de repetição de dados devem ser aplicados em ordem de mais específico a menos específico, se o tráfego encontra critérios múltiplos. Por exemplo, considere este mapa de classe:

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

O tráfego de HTTP deve encontrar o HTTP do protocolo do fósforo primeiramente para certificar-se que o tráfego está segurado pelas capacidades das específicas do serviço de inspeção HTTP. Se as linhas de compatibilidade estão invertidas, assim que o tráfego encontra a indicação tcp do protocolo do fósforo antes que a compare para combinar o HTTP do protocolo, o tráfego está classificado simplesmente como o tráfego TCP, e inspecionado de acordo com as capacidades do componente da inspeção TCP do Firewall. Este é serviços de um problema com certeza tais como o FTP, o TFTP, e os diversos multimédios e serviços da sinalização de voz tais como H.323, o SORVO, o magro, RTSP, e outro. Estes serviços exigem capacidades adicionais da inspeção de reconhecer as atividades mais complexas destes serviços.

Aplicando um ACL como critérios de verificação de repetição de dados

Os mapas de classe podem aplicar um ACL como um dos critérios de verificação de repetição de dados para o aplicativo da política. Se critério do fósforo dos classe-mapas um único é um ACL e o mapa de classe está associado com um mapa de política que aplica a ação da inspeção, o roteador aplica a inspeção básica TCP ou UDP para todo o tráfego permitido pelo ACL, salvo que que ZFW fornece a inspeção aplicativo-ciente. Isto inclui (mas não limitado a) o FTP, o SORVO, o magro (SCCP), H.323, Sun RPC, e TFTP. Se a inspeção característica da aplicação está disponível e o ACL permite o preliminar ou o canal de controle, todo o canal secundário ou dos media associado com o preliminar/controle está permitido, apesar de se o ACL permite o tráfego.

Se um mapa de classe aplica somente o ACL 101 como os critérios de verificação de repetição de dados, um ACL 101 aparece como este:

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

Todo o tráfego é permitido na direção da serviço-política aplicada a um zona-par dado, e o tráfego de retorno correspondente é permitido na direção oposta. Consequentemente, o ACL deve aplicar a limitação para limitar o tráfego aos tipos desejados específico. Note que a lista PAM inclui serviços de aplicativo tais como o HTTP, o NetBIOS, o H.323, e o DNS. Contudo, apesar do conhecimento do PAM do uso do aplicativo específico de uma porta dada, o Firewall aplica somente a suficiente capacidade característica da aplicação de acomodar as exigências conhecidas do tráfego de aplicativo. Assim, o tráfego de aplicativo simples tal como o telnet, o SSH, e outros aplicativos do canal único são inspecionados como o TCP, e suas estatísticas são combinados junto no **show command output (resultado do comando show)**. Se a visibilidade característica da aplicação na atividade de rede é desejada, você precisa de configurar a inspeção para serviços pelo nome do aplicativo (configurar o HTTP do protocolo do fósforo, o telnet do protocolo do fósforo, etc.).

Compare as estatísticas disponíveis no **tipo do mapa de política da mostra inspecionam o** comando dos zona-**pares** output desta configuração com a política de firewall mais explícita mostrada uma pena mais adicional a página. Esta configuração é usada para inspecionar o tráfego de um Cisco IP Phone, assim como diversas estações de trabalho que usam uma variedade de tráfego, que inclui o 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
```

Quando esta configuração for fácil de definir e acomodar todo o tráfego que origina nas portas do destino PAM-reconhecidas privados da zona (enquanto o tráfego observa no padrão,), fornece visibilidade limitada na atividade de serviço, e não oferece a oportunidade de aplicar a largura de banda e os limites de sessão de ZFW para tipos de tráfego específicos. Este **tipo do mapa de política da mostra inspeciona a** saída do comando do priv-**bar dos zona-pares** é o resultado da configuração simples precedente que usa somente um [subnet] da licença IP todo o ACL entre zona-pares. Como você pode ver, a maioria do tráfego da estação de trabalho é contado nas estatísticas básicas 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
```

Pelo contraste, uma configuração similar que adicione classes características da aplicação fornece umas estatísticas e um controle mais granulados do aplicativo, e ainda acomoda a mesma largura dos serviços que foi mostrada no primeiro exemplo definindo o mapa de classe da última oportunidade que combina somente o ACL como a última oportunidade no mapa de política:

```
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 dos mais específico fornece esta saída granulada substancial para o **tipo do mapa de política da mostra inspeciona o** comando do priv-**bar dos zona-pares**:

```
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
```

Um outro benefício adicionado de usar um mapa de classe e uma configuração de mapa de política mais granulados, como mencionada mais cedo, é a possibilidade de aplicar limites classe-específicos na sessão e nos valores de taxa e especificamente de ajustar parâmetros de inspeção aplicando um parâmetro-mapa para ajustar o comportamento da inspeção de cada classe.

Configurando Política-mapas Zona-baseados do Firewall da política

O mapa de política aplica ações da política de firewall a uns ou vários mapas de classe para definir a serviço-política que será aplicada a um zona-par da Segurança. Quando um inspecionar-tipo mapa de política é criado, uma classe padrão nomeada class class-default é aplicada na extremidade da classe. A ação da política padrão dos classe-padrões da classe é gota, mas pode ser mudada para passar. A opção do log pode ser adicionada com a ação de queda. Inspect não pode ser aplicada no class class-default.

Ações Zona-baseadas do Firewall da política

ZFW fornece três ações para o tráfego que atravessa de uma zona a outra:

- **Gota** — Esta é a ação padrão para todo o tráfego, como aplicado pelo “class class-default” que termina cada inspecionar-tipo mapa de política. Outros mapas de classe dentro de um mapa de política podem igualmente ser configurados para deixar cair o tráfego não desejado. Trafique que é segurado pela ação de queda é deixado cair “silenciosamente” (isto é, nenhuma notificação da gota é enviada ao host final relevante) pelo ZFW, ao contrário do comportamento de um ACL de enviar uma mensagem do “host inalcançável” ICMP ao host que enviou o tráfego negado. Atualmente, não há uma opção para mudar “o comportamento da gota silenciosa”. A opção do log pode ser adicionada com gota para a notificação de SYSLOG que o tráfego esteve deixado cair pelo Firewall.
- **Passagem** — Esta ação permite que o roteador envie o tráfego de uma zona a outra. A ação da passagem não segue o estado de conexões ou de sessões dentro do tráfego. A passagem permite somente o tráfego em um sentido. Uma política correspondente deve ser aplicada para permitir que o tráfego de retorno passe na direção oposta. A ação da passagem é útil para protocolos tais como o IPsec ESP, o IPsec AH, o ISAKMP, e outros protocolos inerentemente seguros com comportamento predizível. Contudo, a maioria de tráfego de aplicativo é segurado melhor no ZFW com a ação da inspeção.
- **Inspecione** — As ofertas da ação da inspeção estado-basearam o controle de tráfego. Por exemplo, se o tráfego da zona privada à zona do Internet na rede de exemplo mais adiantada é inspecionado, o roteador mantém a conexão ou a informação de sessão para o tráfego TCP e de User Datagram Protocol (UDP). Consequentemente, o roteador permite o tráfego de retorno enviado dos anfitriões da Internet-zona em resposta aos pedidos de conexão privados da zona. Também, inspecione pode fornecer os protocolos de serviço da inspeção de aplicativo e do controle com certeza que puderam levar o tráfego vulnerável ou do aplicativo sensível. Os circuitos de auditoria podem ser aplicados com um parâmetro-mapa para gravar a conexão/começo da sessão, a parada, a duração, o volume dos dados transferido, e endereços de rementente e destinatário.

As ações são associadas com os mapas de classe nos política-mapas:

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

os Parâmetro-mapas oferecem opções alterar os parâmetros de conexão para uma política da inspeção dos classe-mapas dados.

Configurando Parâmetro-mapas do Firewall da Zona-política

os Parâmetro-mapas especificam o comportamento da inspeção para ZFW, para parâmetros tais como a proteção de DOS, os temporizadores de sessão TCP connection/UDP, e ajustes de registro dos circuitos de auditoria. os Parâmetro-mapas são aplicados igualmente com classe e política-mapas da camada 7 para definir o comportamento característico da aplicação, tal como objetos HTTP, requisitos de autenticação POP3 e IMAP, e a outra informação característica da aplicação.

Os parâmetro-mapas da inspeção para ZFW são configurados como o **tipo inspeciona**, similar à outra classe e aos política-objetos ZFW:

```
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 parâmetro-mapas especificam os parâmetros aplicados por políticas da inspeção de aplicativo da camada 7. o Regex-tipo parâmetro-mapas define uma expressão regular para o uso com inspeção de aplicativo HTTP que os filtros traficam usando uma expressão regular:

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

o Protocolo-informação-tipo parâmetro-mapas define nomes do servidor para o uso com inspeção de aplicativo das mensagens instantâneas:

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

Os detalhes de configuração completos para o HTTP e IM inspeção de aplicativo são fornecidos nas seções da inspeção do aplicativo respectivo deste documento.

Ajustar a proteção de DOS é coberto em uma seção mais recente deste documento.

Configurar a inspeção de aplicativo é coberto em uma seção mais recente deste documento.

Aplicando o registro para políticas de firewall Zona-baseadas da política

ZFW oferece opções de registro para o tráfego que é deixado cair ou inspecionado à revelia ou ações configuradas da política de firewall. O registro dos circuitos de auditoria está disponível para o tráfego que o ZFW inspeciona. Os circuitos de auditoria são aplicados definindo circuitos de auditoria em um parâmetro-mapa e aplicando o parâmetro-mapa com a ação da inspeção em um mapa de política:

```
conf t
```

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

O registro da gota está disponível para o tráfego esse as gotas ZFW. O registro da gota é configurado adicionando o log com a ação de queda em um mapa de política:

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

Editando mapas de classe e Política-mapas do Firewall da Zona-política

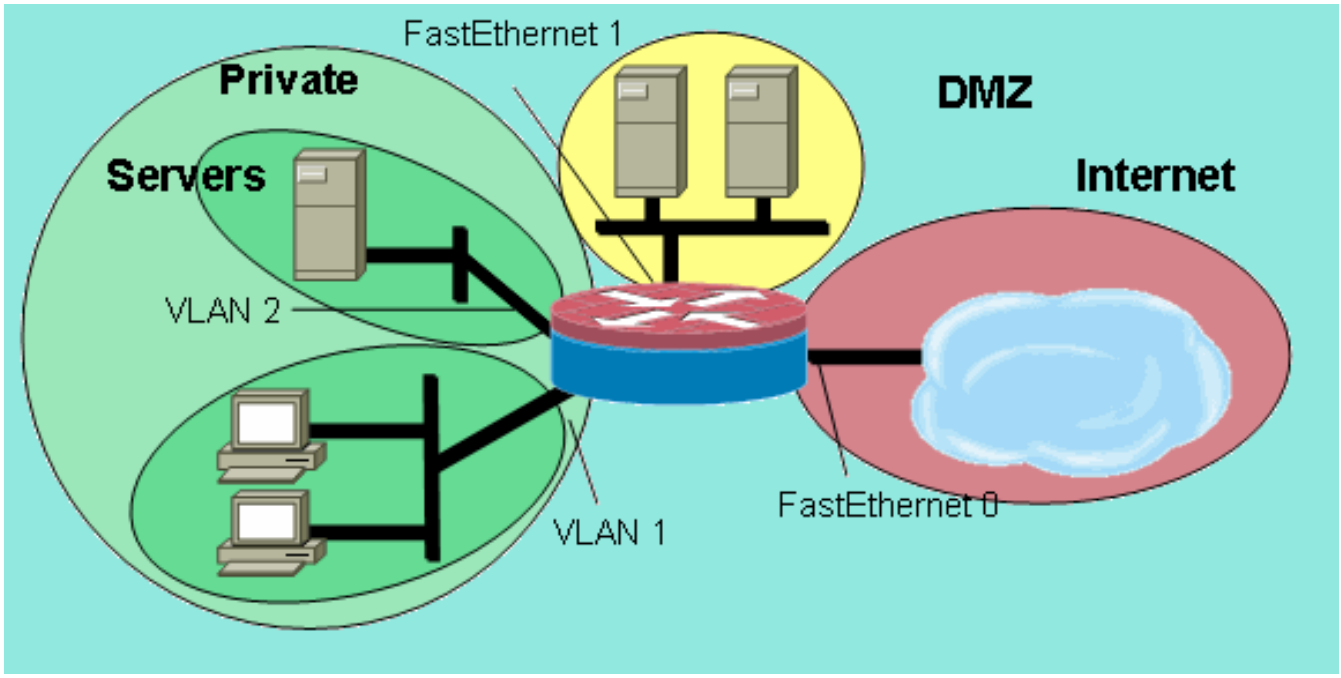
ZFW não incorpora presentemente um editor que possa alterar as várias estruturas ZFW tais como política-mapas, mapas de classe, e parâmetro-mapas. A fim rearranjar instruções compatível em um mapa de classe ou aplicativo da ação aos vários mapas de classe contidos dentro de um mapa de política, você precisa de terminar estas etapas:

1. Copie a estrutura existente a um editor de texto tal como o bloco de notas de Microsoft Windows, ou um editor como vi em Plataformas de Linux/Unix.
2. Remova a estrutura existente da configuração do roteador.
3. Edite a estrutura em seu editor de texto.
4. Copie a estrutura de volta ao CLI do roteador.

Exemplos de configuração

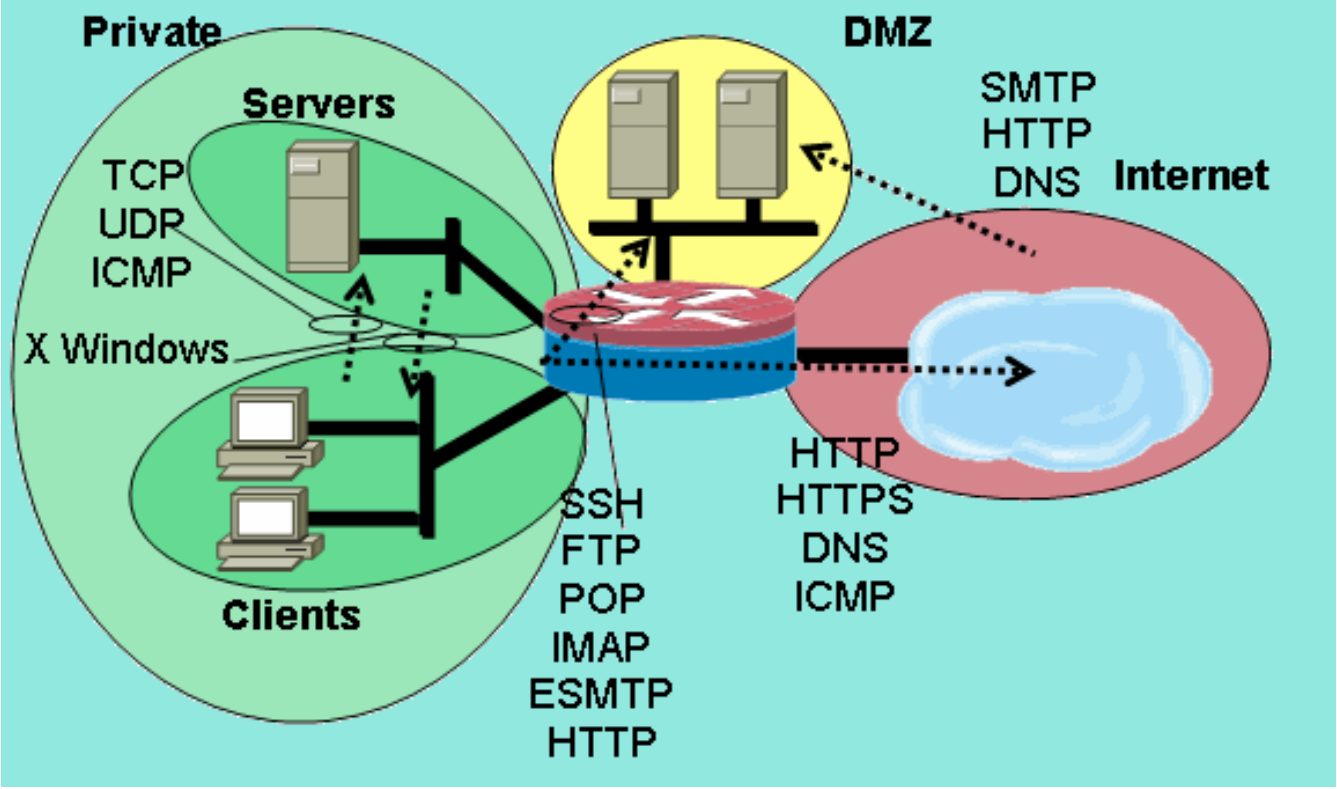
Este exemplo de configuração emprega um Roteador de serviços integrados Cisco 1811. Uma configuração básica com conectividade IP, configuração de VLAN, e Bridging transparente entre dois segmentos privados do LAN de Ethernet está disponível no apêndice A. O roteador é separado em cinco zonas:

- O Internet pública é conectado aos FastEthernet 0 (a zona do Internet)
- Dois servidores de Internet são conectados aos FastEthernet 1 (a zona DMZ)
- O Switch Ethernet é configurado com dois VLAN:As estações de trabalho são conectadas a VLAN1 (zona do cliente).Os server são conectados a VLAN2 (zona do server).As zonas do cliente e servidor estão na mesma sub-rede. Um Firewall transparente será aplicado entre as zonas, assim que as políticas da inter-zona naquelas duas relações afetarão somente o tráfego entre as zonas do cliente e servidor.
- As relações VLAN1 e VLAN2 comunicam-se com outras redes com o Bridge Virtual Interface (BVI1). Esta relação é atribuída à zona privada. (Veja figura 2.)**Figura 2: Detalhe da topologia da zona**



Estas políticas são aplicadas, usando-se as zonas da rede definidas mais cedo:

- Os anfitriões na zona do Internet podem alcançar serviços DNS, S TP, e SSH em um server no DMZ. O outro server oferecerá serviços S TP, HTTP, e HTTPS. A política de firewall restringirá o acesso aos serviços específicos disponíveis em cada host.
- Os anfitriões DMZ não podem conectar aos anfitriões em nenhuma outra zona.
- Os anfitriões na zona do cliente podem conectar aos anfitriões na zona do server em todos os serviços TCP, UDP, e ICMP.
- Os anfitriões na zona do server não podem conectar aos anfitriões na zona do cliente, a não ser que um server de aplicativo baseado no Unix possa abrir sessões cliente do X Windows aos server do X Windows no desktop PC na zona do cliente nas portas 6900 6910.
- Todos os anfitriões na zona privada (combinação de clientes e servidor) podem alcançar anfitriões no DMZ em serviços SSH, FTP, POP, IMAP, ESMTP, e HTTP, e na zona do Internet em serviços HTTP, HTTPS, e DNS e em ICMP. Além disso, a inspeção de aplicativo será aplicada em conexões de HTTP da zona privada à zona do Internet a fim assegurar que as mensagens instantâneas apoiadas e os aplicativos P2P não são a porta continuada 80. (Veja figura 3.)**Figura 3: Permissões do serviço dos Zona-pares ser aplicado no exemplo de configuração**



Estas políticas de firewall são configuradas por ordem da complexidade:

1. Inspeção dos Cliente-server TCP/UDP/ICMP
2. Inspeção Privado-DMZ SSH/FTP/POP/IMAP/ESMTP/HTTP
3. Internet - Inspeção DMZ SMTP/HTTP/DNS restringida pelo endereço de host
4. Inspeção do X Windows dos Server-clientes com um mapeamento da porta de aplicativo (PAM) - serviço especificado
5. Internet privadas HTTP/HTTPS/DNS/ICMP com inspeção de aplicativo HTTP

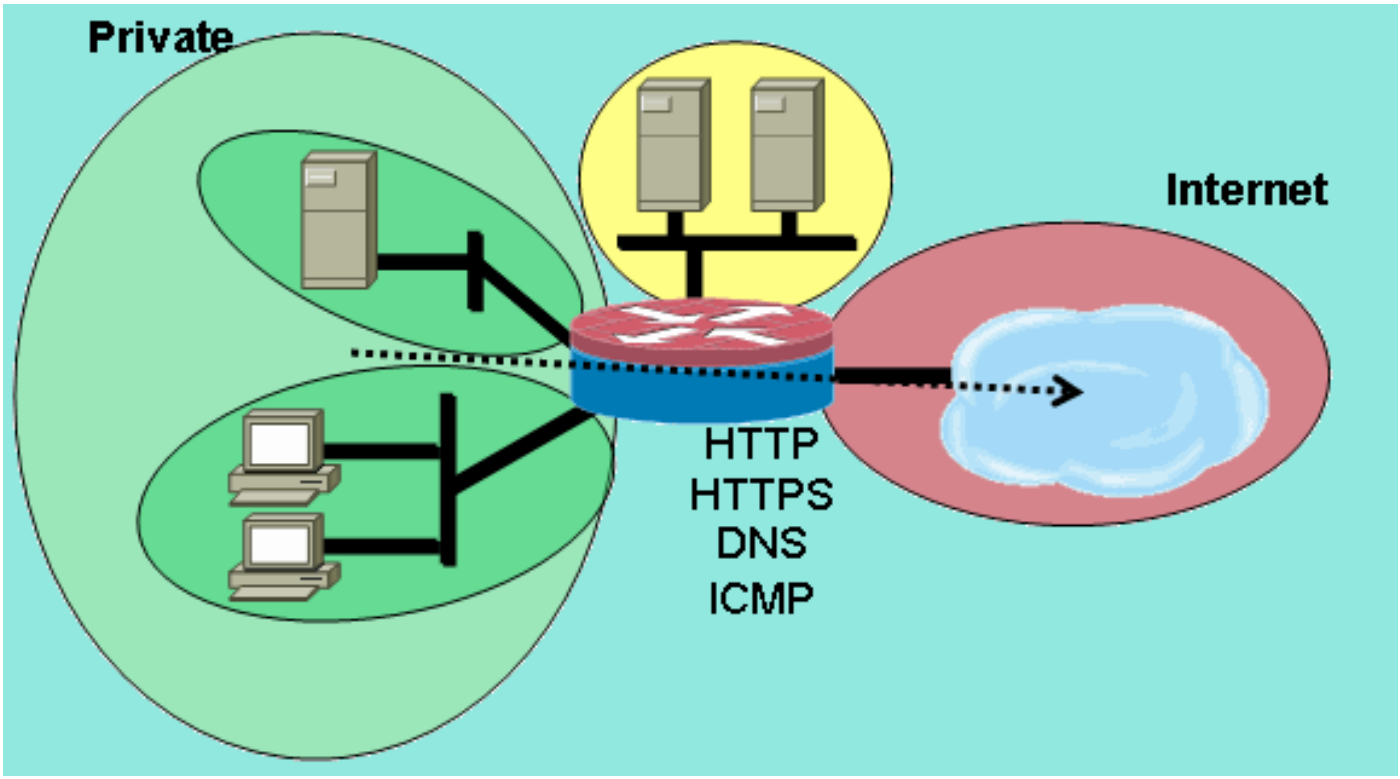
Porque você aplicará parcelas da configuração aos segmentos de rede diferentes em horas diferentes, é importante recordar que um segmento de rede perderá a Conectividade a outros segmentos quando é colocado em uma zona. Por exemplo, quando a zona privada é configurada, os anfitriões na zona privada perderão a Conectividade às zonas DMZ e de Internet até que suas políticas respectivas estejam definidas.

Firewall do roteamento da inspeção stateful

Configurar a política das Internet privadas

Figura 4 ilustra a configuração da política das Internet privadas.

Figura 4: Inspeção de serviço da zona privada à zona do Internet



A política das Internet privadas aplica a inspeção da camada 4 ao HTTP, HTTPS, DNS, e mergulha a inspeção 4 para o ICMP da zona privada à zona do Internet. Isto permite conexões da zona privada à zona do Internet, e permite o tráfego de retorno. A inspeção da camada 7 leva as vantagens de um controle de aplicativo mais apertado, da melhor Segurança, e do apoio para os aplicativos que exigem reparares. Contudo, a inspeção da camada 7, como mencionada, exige uma compreensão melhor da atividade de rede, como os protocolos da camada 7 que não são configurados para a inspeção não serão permitidos entre zonas.

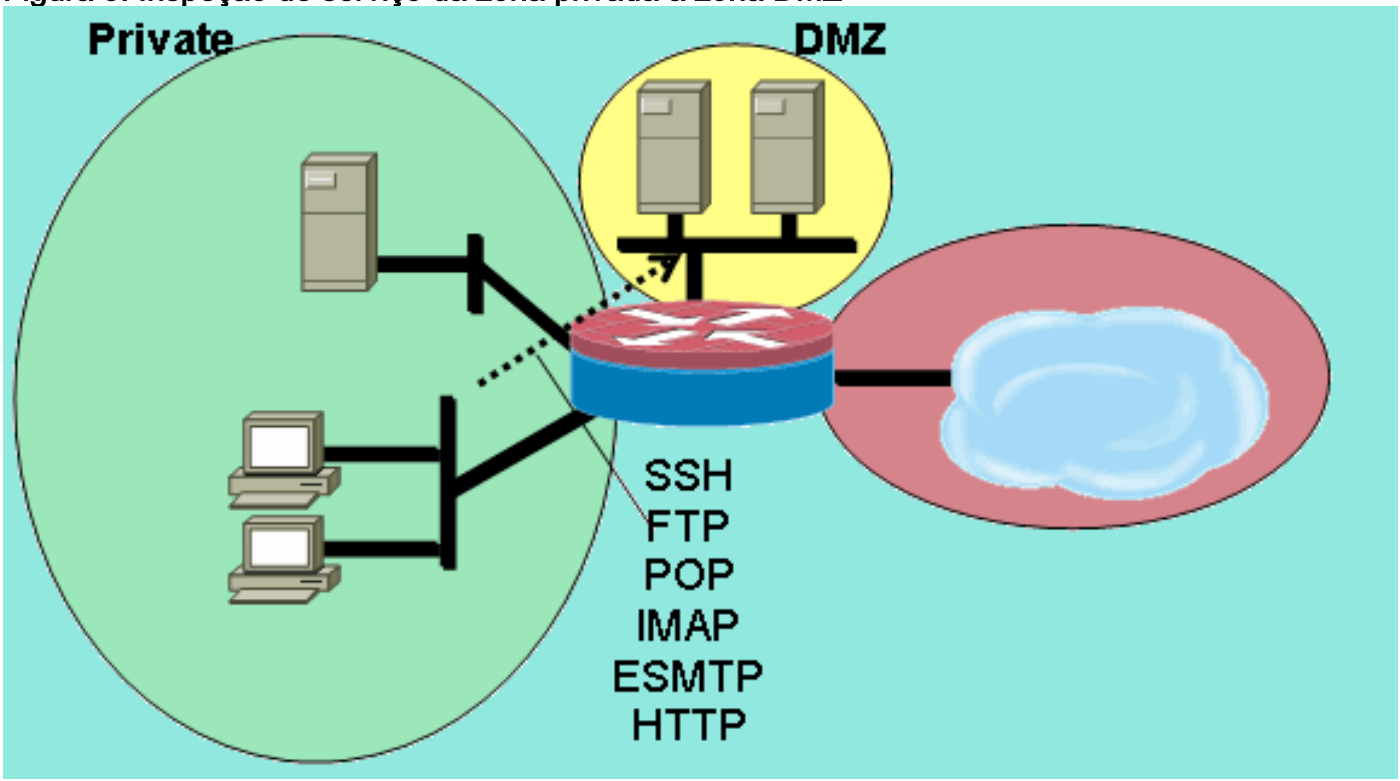
1. Defina os mapas de classe que descrevem o tráfego que você quer permitir entre zonas, de acordo com as políticas descritas mais cedo:`conf t`
```
 class-map type inspect match-any internet-traffic-class
  match protocol http
  match protocol https
  match protocol dns
  match protocol icmp
```
2. Configurar um mapa de política para inspecionar o tráfego nos mapas de classe que você apenas definiu:`conf t`
```
 policy-map type inspect private-internet-policy
  class type inspect internet-traffic-class
   inspect
```
3. Configurar as zonas privadas e do Internet e atribua interfaces do roteador a suas zonas respectivas:`conf t`
```
zone security private
zone security internet
int bvi1
zone-member security private
int fastethernet 0
zone-member security internet
```
4. Configurar os zona-pares e aplique o mapa de política apropriado.**Nota:** Você precisa somente de configurar presentemente os pares da zona das Internet privadas a fim inspecionar as conexões originado na zona privada que viaja à zona do Internet:`conf t`
```
 zone-pair security private-internet source private destination internet
  service-policy type inspect private-internet-policy
```
Isto termina a configuração da política

da inspeção da camada 7 nos zona-pares das Internet privadas para permitir conexões HTTP, HTTPS, DNS, e ICMP da zona dos clientes à zona dos server e para aplicar a inspeção de aplicativo ao tráfego de HTTP para assegurar que o tráfego não desejado não está permitido passar sobre TCP 80, porta do serviço do HTTP.

Configurar a política privada DMZ

A figura 5 ilustra a configuração da política privada DMZ.

Figura 5: Inspeção de serviço da zona privada à zona DMZ



A política privada DMZ adiciona a complexidade porque exige uma compreensão melhor do tráfego de rede entre zonas. Esta política aplica a inspeção da camada 7 da zona privada ao DMZ. Isto permite conexões da zona privada ao DMZ, e permite o tráfego de retorno. A inspeção da camada 7 leva as vantagens de um controle de aplicativo mais apertado, da melhor Segurança, e do apoio para os aplicativos que exigem reparares. Contudo, a inspeção da camada 7, como mencionada, exige uma compreensão melhor da atividade de rede, como os protocolos da camada 7 que não são configurados para a inspeção não serão permitidos entre zonas.

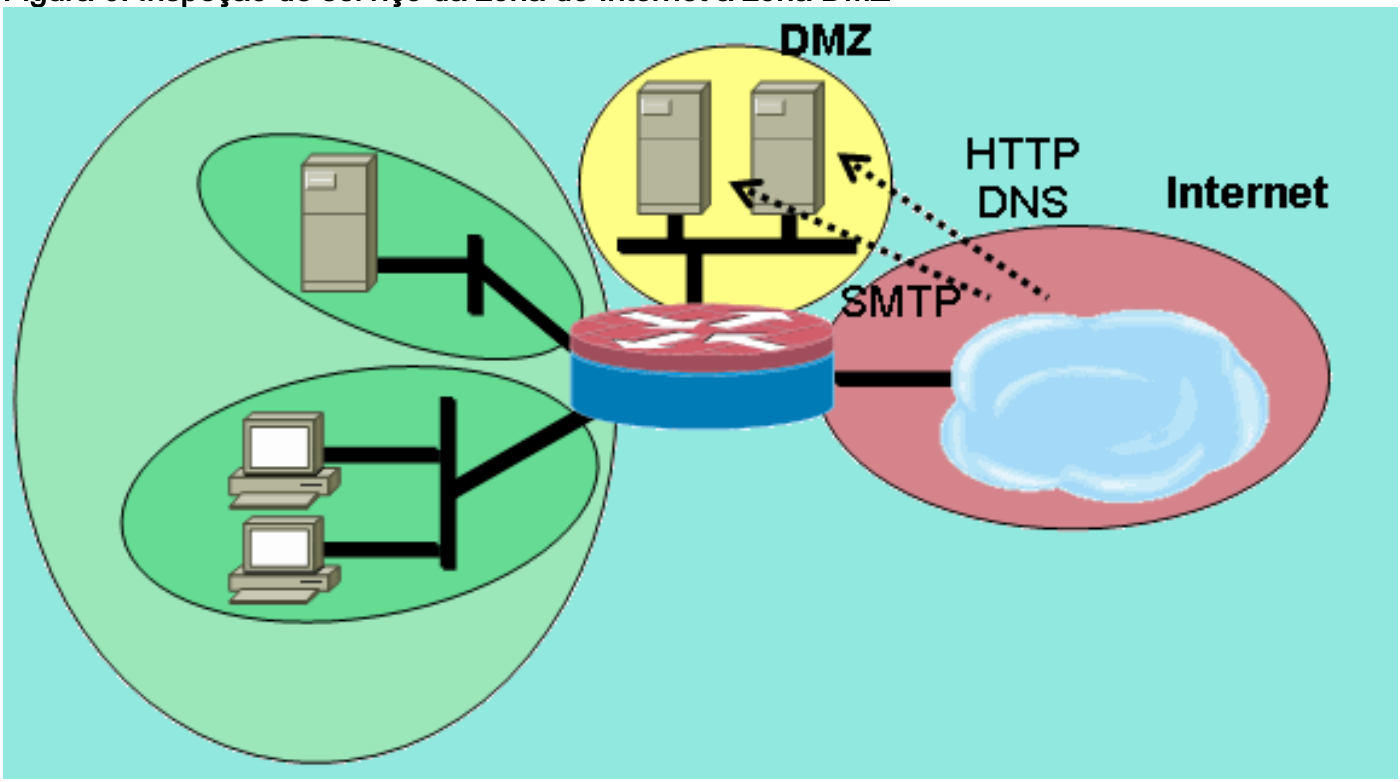
1. Defina os mapas de classe que descrevem o tráfego que você quer permitir entre zonas, de acordo com as políticas descritas mais cedo:`conf t`
```
 class-map type inspect match-any L7-inspect-class
  match protocol ssh
  match protocol ftp
  match protocol pop
  match protocol imap
  match protocol esmtp
  match protocol http
```
2. Configurar política-mapas para inspecionar o tráfego nos mapas de classe que você apenas definiu:`conf t`
```
 policy-map type inspect private-dmz-policy
  class type inspect L7-inspect-class
   inspect
```

3. Configurar as zonas privadas e DMZ e atribua interfaces do roteador a suas zonas respectivas:
```
conf t
zone security private
zone security dmz
int bvi1
zone-member security private
int fastethernet 1
zone-member security dmz
```
4. Configurar os zona-pares e aplique o mapa de política apropriado.**Nota:** Você precisa somente de configurar presentemente os zona-pares privados DMZ a fim inspecionar as conexões originado na zona privada que viaja ao DMZ:
```
conf t
 zone-pair security private-dmz source private destination dmz
  service-policy type inspect private-dmz-policy
```
Isto termina a configuração da política da inspeção da camada 7 no DMZ privado para permitir todas as conexões TCP, UDP, e ICMP da zona dos clientes à zona dos server. A política não aplica reparares para os canais subordinados, mas fornece um exemplo da política simples para acomodar a maioria de conexões do aplicativo.

Configurar a política do Internet DMZ

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

Figura 6: Inspeção de serviço da zona do Internet à zona DMZ



Esta política aplica a inspeção da camada 7 da zona do Internet ao DMZ. Isto permite conexões da zona do Internet ao DMZ, e permite o tráfego de retorno dos anfitriões DMZ aos host de Internet que originaram a conexão. A política do Internet DMZ combina a inspeção da camada 7 com os grupos de endereço definidos por ACL para restringir o acesso aos serviços específicos em anfitriões específicos, aos grupos de anfitriões, ou às sub-redes. Isto é realizado aninhando um mapa de classe que especifica serviços dentro de um outro mapa de classe que provê um ACL para especificar endereços IP de Um ou Mais Servidores Cisco ICM NT.

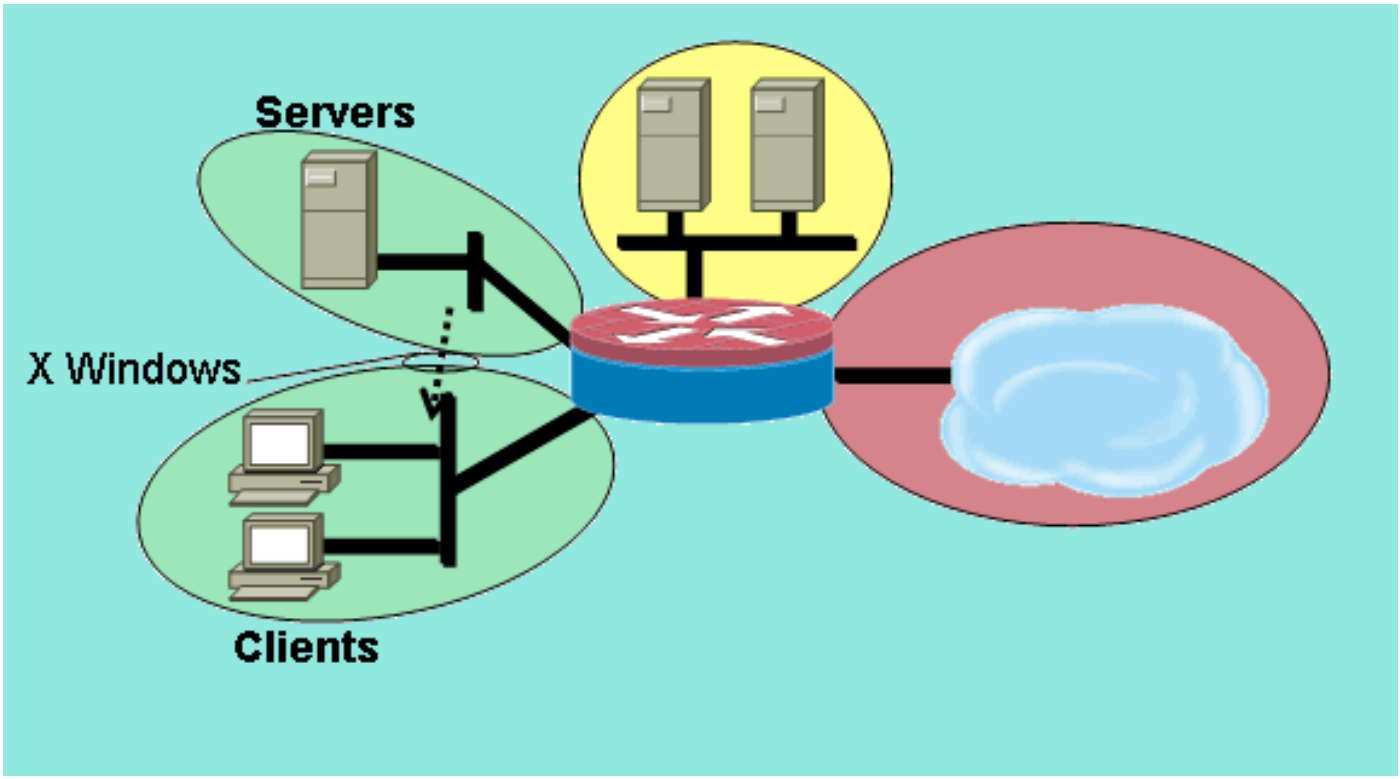
1. Defina os mapas de classe e os ACL que descrevem o tráfego que você quer permitir entre zonas, de acordo com as políticas descritas mais cedo.Os mapas de classe múltiplos para serviços devem ser usados, porque as políticas de acesso de deferimento serão aplicadas para o acesso a dois server diferentes. Os host de Internet são permitidas o DNS e as conexões de HTTP a 172.16.2.2, e as conexões SMTP são permitidas a 172.16.2.3. Note a diferença nos mapas de classe. Os mapas de classe que especificam serviços usam a palavra-chave **compatível com qualquer** para permitir alguns dos serviços listados. Os mapas de classe que associam ACL com os mapas de classe do serviço usam a palavra-chave **compatível com todos** para exigir que ambas as condições no mapa da classe devem ser estadas conformes para permitir o tráfego:`conf t`
```
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 política-mapas para inspecionar o tráfego nos mapas de classe que você apenas definiu:`conf t`
```
policy-map type inspect internet-dmz-policy
 class type inspect dns-http-acl-class
  inspect
 class type inspect smtp-acl-class
  inspect
```
3. Configurar o Internet e zonas DMZ e atribua interfaces do roteador a suas zonas respectivas. Salte a configuração DMZ se você a ajusta acima na seção anterior:`conf t`
```
zone security internet
zone security dmz
int fastethernet 0
 zone-member security internet
int fastethernet 1
 zone-member security dmz
```
4. Configurar os zona-pares e aplique o mapa de política apropriado.**Nota:** Você precisa somente de configurar presentemente os pares da zona do Internet DMZ, para inspecionar as conexões originado na zona do Internet que viaja à zona DMZ:`conf t`
```
zone-pair security internet-dmz source internet destination dmz
 service-policy type inspect internet-dmz-policy
```
Isto termina a configuração da política endereço-específica da inspeção da camada 7 nos zona-pares do Internet DMZ.

Firewall transparente da inspeção stateful

Configurar a política dos Server-clientes

A figura 7 ilustra a configuração da política do server-cliente.

Figura 7: Inspeção de serviço da zona dos server à zona dos clientes



A política dos server-clientes aplica a inspeção usando um serviço definido pelo utilizador. A inspeção da camada 7 é aplicada da zona dos server à zona dos clientes. Isto permite conexões do X Windows a um intervalo de porta específico da zona dos server à zona dos clientes, e permite o tráfego de retorno. O X Windows não é nativamente um protocolo suportado no PAM, assim que um serviço do configurado pelo usuário no PAM deve ser definido assim que o ZFW pode reconhecer e inspecionar o tráfego apropriado.

Dois ou mais interfaces do roteador são configuradas em um ponte-grupo da IEEE para fornecer o Integrated Routing and Bridging (IRB) para fornecer a construção de uma ponte sobre entre as relações no ponte-grupo e a distribuição a outras sub-redes através do Bridge Virtual Interface (BVI). A política de firewall transparente oferecerá aplica a inspeção do Firewall para o tráfego “que cruza a ponte”, mas não para o tráfego que deixa o ponte-grupo através do BVI. A política da inspeção aplica-se somente para traficar cruzando o ponte-grupo. Consequentemente, nesta encenação, a inspeção será aplicada somente para traficar que movimentos entre as zonas dos clientes e servidor, que são aninhadas dentro da zona privada. A política aplicada entre a zona privada, e o público e as zonas DMZ, entram somente o jogo quando o tráfego deixa o ponte-grupo através do BVI. Quando o tráfego sae através do BVI dos clientes ou das zonas dos server, a política de firewall transparente não estará invocada.

1. Configurar o PAM com uma entrada definida pelo utilizador para o X Windows.Conexões aberta dos clientes do X Windows (onde os aplicativos são hospedados) para o Exibir informação aos clientes (onde o usuário está trabalhando) em uma escala que começa na porta 6900.Cada conexão adicional usa portas sucessivas, assim que se um cliente indica as sessões 10 diferentes em um host, o server usa portas 6900-6909. Consequentemente, se você inspeciona o intervalo de porta de 6900 a 6909, as conexões abertas às portas além de 6909 falharão:`conf t`
   ```
   ip port-map user-Xwindows port tcp from 6900 to 6910
   ```
2. Reveja documentos PAM para endereçar perguntas adicionais PAM ou para verificar a documentação granulada da inspeção do protocolo para obter informações sobre dos detalhes de Interoperabilidade entre o PAM e a inspeção stateful do Cisco IOS Firewall.
3. Defina os mapas de classe que descrevem o tráfego que você quer permitir entre zonas, de

acordo com as políticas descritas mais cedo:`conf t`

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

4. Configurar política-mapas para inspecionar o tráfego nos mapas de classe que você apenas definiu:`conf t`

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

5. Configurar as zonas do cliente e servidor e atribua interfaces do roteador a suas zonas respectivas.Se você configurou estas zonas e atribuiu relações na seção de configuração das normas dos Cliente-server, você pode saltar à definição dos zona-pares. Construir uma ponte sobre a configuração de IRB é fornecida para a integralidade:`conf t`

```
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. Configurar os zona-pares e aplique o mapa de política apropriado.**Nota:** Você precisa somente de configurar presentemente os pares da zona dos server-clientes a fim inspecionar as conexões originado na zona dos server que viaja à zona dos clientes:`conf t`

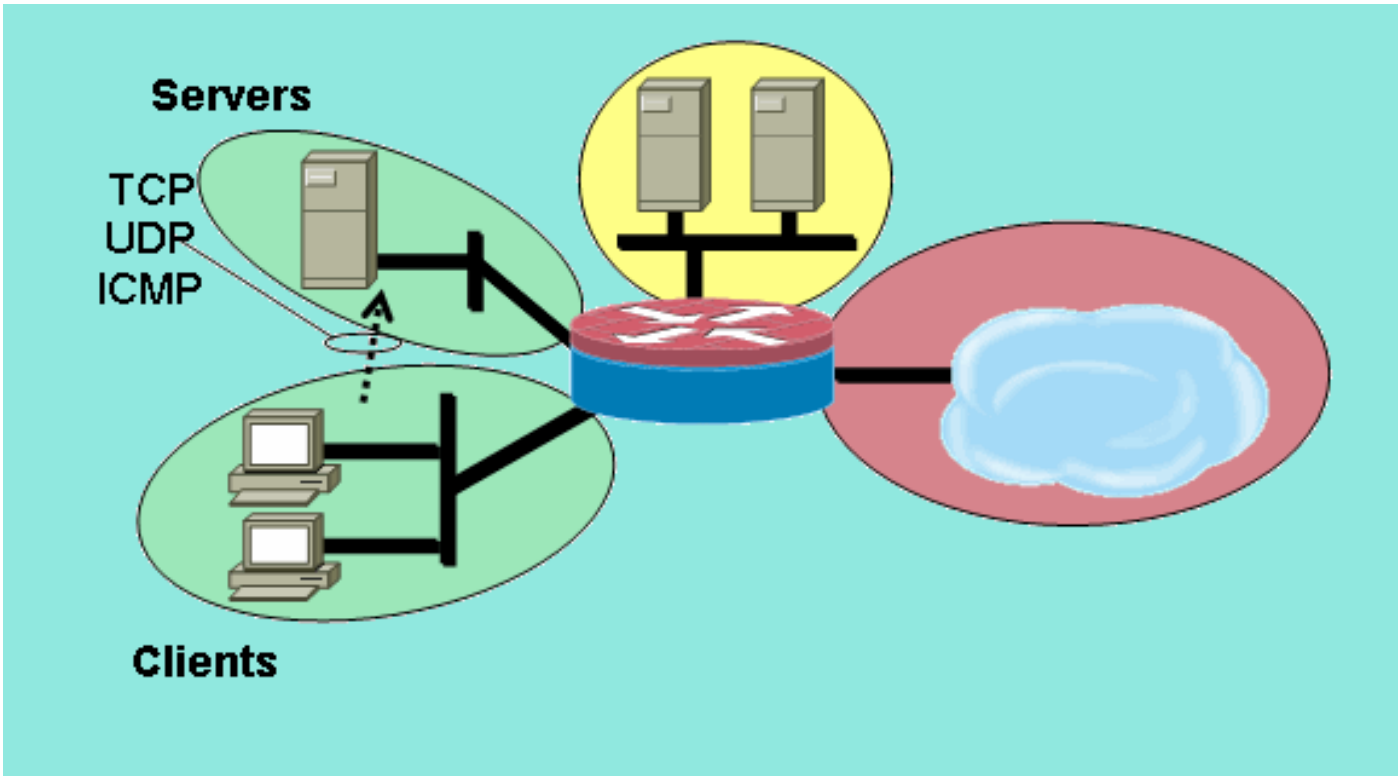
```
 zone-pair security servers-clients source servers destination clients
  service-policy type inspect servers-clients-policy
```

Isto termina a configuração da política definida pelo utilizador da inspeção nos zona-pares dos server-clientes para permitir conexões do X Windows da zona do server à zona do cliente.

Configurar a política dos Cliente-server

Figura 8 ilustra a configuração da política do servidor cliente.

Figura 8: Inspeção de serviço da zona dos clientes à zona dos server



A política dos servidores cliente é menos complexa do que a outro. A inspeção da camada 4 é aplicada da zona dos clientes à zona dos server. Isto permite conexões da zona dos clientes à zona dos server, e permite o tráfego de retorno. A inspeção da camada 4 leva a vantagem da simplicidade na configuração de firewall, que somente algumas regras estão exigidas para permitir a maioria de tráfego de aplicativo. Contudo, a inspeção da camada 4 igualmente leva duas desvantagens principais:

- Os aplicativos tais como o FTP ou os serviços de mídia fluente negociam frequentemente um canal subordinado adicional do server ao cliente. Esta funcionalidade é acomodada geralmente em um reparar do serviço que monitore o diálogo do canal de controle e permita o canal subordinado. Esta capacidade não está disponível na inspeção da camada 4.
- A inspeção da camada 4 permite quase todo o tráfego da camada de aplicativo. Se o uso da rede deve ser controlado tão somente alguns aplicativos estão permitidos com o Firewall, um ACL devem ser configurados no tráfego de saída para limitar os serviços permitidos com o Firewall.

Ambas as interfaces do roteador são configuradas em um grupo de bridge da IEEE, assim que esta política de firewall aplicará a inspeção transparente do Firewall. Esta política é aplicada em duas relações em um grupo de bridge IP da IEEE. A política da inspeção aplica-se somente para traficar cruzando o grupo de bridge. Isto explica porque as zonas dos clientes e servidor são aninhadas dentro da zona privada.

1. Defina os mapas de classe que descrevem o tráfego que você quer permitir entre zonas, de acordo com as políticas descritas mais cedo:`conf t`
```
class-map type inspect match-any L4-inspect-class
match protocol tcp
match protocol udp
match protocol icmp
```
2. Configurar política-mapas para inspecionar o tráfego nos mapas de classe que você apenas definiu:`conf t`
```
policy-map type inspect clients-servers-policy
class type inspect L4-inspect-class
 inspect
```

3. Configurar as zonas dos clientes e servidor e atribua interfaces do roteador a suas zonas respectivas:
```
conf t
zone security clients
zone security servers
int vlan 1
zone-member security clients
int vlan 2
zone-member security servers
```
4. Configurar os zona-pares e aplique o mapa de política apropriado.**Nota:** Você precisa somente de configurar presentemente os zona-pares dos cliente-server, para inspecionar as conexões originado na zona dos clientes que viaja à zona dos server:
```
conf t
 zone-pair security clients-servers source clients destination servers
  service-policy type inspect clients-servers-policy
```
Isto termina a configuração da política da inspeção da camada 4 para que os zona-pares dos cliente-server permitam todas as conexões TCP, UDP, e ICMP da zona do cliente à zona do server. A política não aplica reparares para os canais subordinados, mas fornece um exemplo da política simples para acomodar a maioria de conexões do aplicativo.

Taxa que policia para o Firewall Zona-baseado da política

As redes de dados beneficiam-se frequentemente com a capacidade para limitar a taxa de transmissão de tipos de rede específicos traficam, e para limitar o impacto do tráfego de prioridade mais baixa a um tráfego negócio-mais essencial. O Cisco IOS Software oferece esta capacidade com Policiamento de tráfego, que a taxa nominal e a explosão do tráfego dos limites. O Cisco IOS Software apoiou o Policiamento de tráfego desde o Cisco IOS Release 12.1(5)T.

O Cisco IOS Software Release 12.4(9)T aumenta ZFW com a taxa limite adicionando a capacidade de policiar o tráfego que combina as definições de um mapa de classe específico enquanto atravessa o Firewall de uma zona de Segurança a outra. Isto fornece a conveniência de oferecer um ponto da configuração descrever o tráfego específico, para aplicar a política de firewall, e a polícia o consumo de largura de banda desse tráfego. O policiamento ZFW difere do policiamento relação-baseado que fornece somente as ações transmite para a conformidade e a gota da política para a violação da política. O policiamento ZFW não pode marcar o tráfego para o DSCP.

O policiamento ZFW pode somente especificar o uso da largura de banda nos bytes/em segundo, pacote/em segundo e o policiamento do percentual de largura de banda não é oferecido. O policiamento ZFW pode ser aplicado com ou sem o policiamento relação-baseado. Consequentemente, se as capacidades de policiamento adicionais são exigidas, estas características podem ser aplicadas pelo policiamento relação-baseado. Se o policiamento relação-baseado é usado conjuntamente com o Firewall que policia, assegure que as políticas não oponham.

Configurando o policiamento ZFW

ZFW que policiam limites traficam em um mapa de classe dos política-mapas a um valor de taxa definido pelo utilizador entre 8,000 e 2,000,000,000 bit por segundo, com um valor de intermitência configurável na escala de 1,000 a 512,000,000 bytes.

O policiamento ZFW é configurado por uma linha adicional de configuração no mapa de política, que é aplicada após a ação de 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

ZFW que policia o controle de sessão igualmente introduzido para limitar o contagem de sessão para o tráfego em um mapa de política que combina um mapa de classe. Isto adiciona à capacidade existente de aplicar a política da proteção de DOS pelo mapa de classe. Eficazmente, isto permite o controle granulado no número de sessões que combinam todo o mapa de classe dado que cruzam um zona-par. Se o mesmo mapa de classe é usado em política-mapas múltiplos ou em zona-pares, os limites de sessão diferentes podem ser aplicados nos vários aplicativos do mapa de classe.

O controle de sessão é aplicado configurando um parâmetro-mapa que contenha o volume desejado da sessão, adicionando então o parâmetro-mapa à ação da inspeção aplicada a um mapa de classe sob um mapa de política:

```
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 Parâmetro-mapas podem somente ser aplicados à ação da inspeção, e não estão disponíveis na passagem ou nas ações de queda.

O controle de sessão de ZFW e as atividades do policiamento são visíveis com este comando

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

Inspeção de aplicativo

A inspeção de aplicativo introduz a capacidade adicional a ZFW. As políticas da inspeção de aplicativo são aplicadas na camada 7 do modelo osi, onde os aplicativos de usuário enviam e recebem as mensagens que permitem os aplicativos oferecer capacidades úteis. Alguns aplicativos puderam oferecer capacidades indesejadas ou vulneráveis, assim que as mensagens associadas com estas capacidades devem ser filtradas para limitar atividades nos serviços de aplicativo.

O Cisco IOS Software ZFW oferece a inspeção de aplicativo e o controle nestes serviços de aplicativo:

- HTTP
- SMTP
- POP3
- IMAP
- Sun RPC
- Tráfego de aplicativo P2P
- IM aplicativos

A inspeção de aplicativo e o controle (AIC) variam na capacidade pelo serviço. A inspeção HTTP oferece a filtração granulada em diversos tipos de atividade do aplicativo, oferecendo capacidades de limitar o tamanho de transferência, comprimentos do endereço de web, e

atividade do navegador para reforçar a conformidade com padrões do comportamento de aplicativo e para limitar os tipos de índice que são transferidos sobre o serviço. O AIC para o S TP pode limitar o comprimento satisfeito e reforçar a conformidade do protocolo. A inspeção POP3 e IMAP pode ajudar a assegurar-se de que os usuários se estejam usando fixem mecanismos da autenticação para impedir o acordo de credenciais do usuário.

A inspeção de aplicativo é configurada como um grupo adicional de mapas de classe e de política-mapas característicos da aplicação, que são aplicados então aos mapas de classe e aos política-mapas existentes da inspeção definindo a política de serviços de aplicativo no mapa de política da inspeção.

Inspeção de aplicativo HTTP

A inspeção de aplicativo pode ser aplicada no tráfego de HTTP para controlar uso indesejável da porta do serviço do HTTP para outros aplicativos tais como o compartilhamento de arquivo de IM, P2P, e os aplicativos do Tunelamento que podem reorientar aplicativos de outra maneira firewalled com TCP 80.

Configurar um mapa de classe da inspeção de aplicativo para descrever o tráfego que viola o tráfego de 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
```

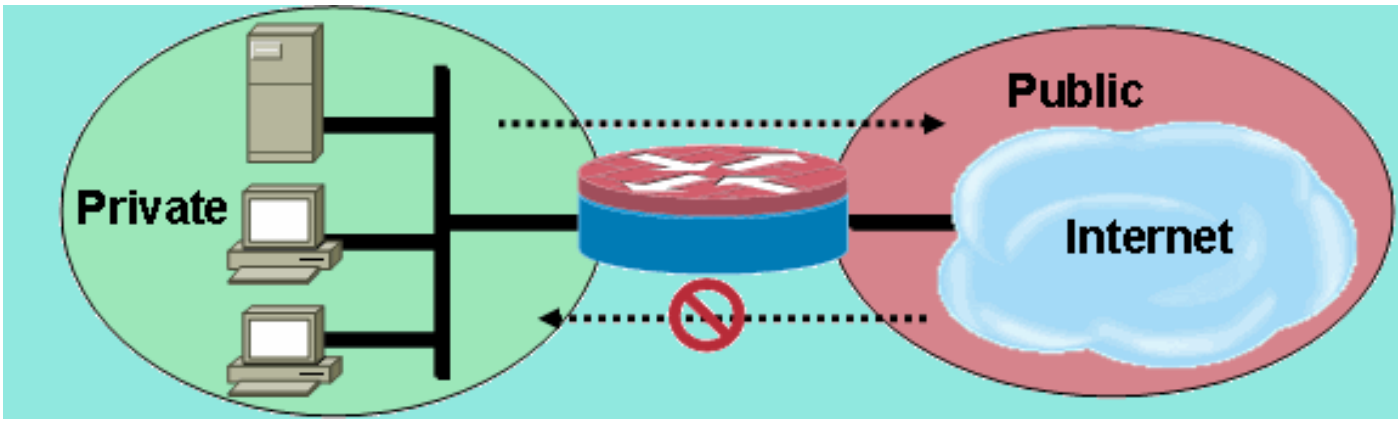
Melhorias da inspeção de aplicativo HTTP

O Cisco IOS Software Release 12.4(9)T introduz melhorias às capacidades da inspeção HTTP de ZFW. Inspeção de aplicativo introduzida Cisco IOS Firewall HTTP no Cisco IOS Software Release 12.3(14)T. O Cisco IOS Software Release 12.4(9)T aumenta capacidades existentes adicionando:

- A capacidade para permitir, nega, e monitora os pedidos e as respostas baseados no nome e nos valores de cabeçalho do encabeçamento. Isto é útil obstruir os pedidos e as respostas que levam campos de cabeçalho vulneráveis.
- Capacidade para limitar os tamanhos de elementos diferentes no pedido do HTTP e nos

cabeçalhos da resposta tais como o comprimento máximo URL, o comprimento de cabeçalho máximo, o número máximo de encabeçamentos, o comprimento de linha de cabeçalho máximo, etc. Isto é útil impedir excessos de buffer.
- Capacidade para obstruir pedidos e respostas que levam encabeçamentos múltiplos do mesmo tipo; por exemplo, um pedido com os dois encabeçamentos do índice-comprimento.
- Capacidade para obstruir pedidos e respostas com os encabeçamentos NON-ASCII. Isto é útil impedir os vários ataques que usam o binário e os outros caráteres NON-ASCII para entregar worms e outros índices maliciosos aos servidores de Web.
- A capacidade para agrupar métodos HTTP em categorias especificadas pelo utilizador e a flexibilidade obstruir/reservam/monitores que cada um do grupo é oferecido. O HTTP RFC permite um grupo restrito de métodos HTTP. Alguns dos métodos padrão são considerados inseguros porque podem ser usadas para explorar vulnerabilidades em um servidor de Web. Muitos dos métodos não padronizados têm um registro ruim da Segurança.
- Método para obstruir os URI específicos baseados em uma expressão regular do configurado pelo usuário. Esta característica dá a um usuário a capacidade de obstruir o costume URI e as perguntas.
- A capacidade ao encabeçamento do spoof datilografa (especialmente tipo do encabeçamento do server) com cordas customizáveis do usuário. Isto é útil em um caso onde um atacante analise respostas do servidor de Web e aprenda tanta informação como possível, a seguir lança um ataque que explore fraquezas nesse servidor particular da Web.
- Capacidade para obstruir ou emitir um alerta em uma conexão de HTTP se uns ou vários valores de parâmetro HTTP combinam os valores incorporados pelo usuário como uma expressão regular. Alguns dos contextos possíveis do valor HTTP incluem o encabeçamento, o corpo, o username, a senha, o agente de usuário, a linha do pedido, a linha de status, e variáveis descodificadas CGI.

Os exemplos de configuração para melhorias da inspeção de aplicativo HTTP supõem uma rede simples:



O Firewall agrupa o tráfego em duas classes:

- Tráfego de HTTP
- Todo canal único restante TCP, tráfego UDP, e ICMP

O HTTP é separado para permitir a inspeção específica no tráfego de web. Isto permite que você configurem o policiamento na primeira seção deste documento, e a inspeção de aplicativo HTTP na segunda seção. Você configurará mapas de classe e política-mapas específicos para o P2P e IM tráfego na terceira seção deste documento. A Conectividade é permitida da zona privada à zona pública. Nenhuma Conectividade é fornecida da zona pública à zona privada.

Uma configuração completa que executa a política inicial é fornecida no C do apêndice, configuração de firewall básica da Zona-política para duas zonas.

Configurando realces da inspeção de aplicativo HTTP

A inspeção de aplicativo HTTP (assim como outras políticas da inspeção de aplicativo) exigem mais configuração complexa do que a configuração da camada básica 4. Você deve configurar a Classificação de tráfego e a política da camada 7 para reconhecer o tráfego específico que você deseja controlar, e para aplicar a ação desejada ao tráfego desejável e indesejável.

A inspeção de aplicativo HTTP (similar a outros tipos de inspeção de aplicativo) pode somente ser aplicada ao tráfego de HTTP. Assim, você deve definir mapas de classe e política-mapas da camada 7 para o tráfego de HTTP específico, a seguir define um mapa de classe Layer-4 especificamente para o HTTP, e aplica a política Layer-7 à inspeção HTTP em um mapa de política Layer-4, como esta':

```
!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 estas características de tráfego da inspeção de aplicativo HTTP são definidas em um mapa de classe da camada 7:

- **Inspeção do encabeçamento** — Este comando fornece a capacidade para permitir/nega-a/a pedido ou respostas do monitor cujo o encabeçamento combina a expressão regular configurada. Reserve ou restaurar a ação pode ser aplicada a um pedido ou a uma resposta que combinam os critérios do mapa de classe. A adição da ação do log causa um mensagem do syslog:`APPFW-6-HTTP_HDR_REGEX_MATCHED`*Comando usage:*`match {request|response|req-resp} header regex <parameter-map-name>` *Caso do uso da amostra*Configurar uma política do appfw HTTP para obstruir o pedido ou a resposta cujo o encabeçamento contém os caráteres NON-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
```
- **Inspeção do comprimento de cabeçalho** — Este comando verifica o comprimento de um

pedido ou de um cabeçalho da resposta e aplica a ação se o comprimento excede o limiar configurado. A ação é reserva ou restaura. A adição da ação do log causa um mensagem do syslog:`APPFW-4- HTTP_HEADER_LENGTH`*Comando usage:*`match {request|response|req-resp} header length gt <bytes>` *Caso do uso da amostra*Configurar uma política do appfw HTTP para obstruir os pedidos e as respostas que têm maiores de 4096 bytes do comprimento de cabeçalho.

```
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
```

- **Inspeção da contagem do encabeçamento** — Este comando verifica o número de linhas de cabeçalho (campos) em um pedido/resposta e aplica a ação quando a contagem excede o limiar configurado. A ação é reserva ou restaura. A adição da ação do log causa um mensagem do syslog:`APPFW-6- HTTP_HEADER_COUNT.`*Comando usage:*`match {request|response|req-resp} header count gt <number>` *Caso do uso da amostra*Configurar uma política do appfw HTTP para obstruir um pedido que tenha 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
```

- **Inspeção de campo de cabeçalho** — Este comando fornece a capacidade para permitir/nega-a/pedido/respostas do monitor que contêm um campo de cabeçalho HTTP específico e o avaliam. Reserve ou restaurar a ação pode ser aplicada a um pedido ou a uma resposta que combinam os critérios do mapa de classe. A adição da ação do log causa um mensagem do syslog:`APPFW-6- HTTP_HDR_FIELD_REGEX_MATCHED`*Comando usage:*`match {request|response|req-resp} header <header-name>` *Caso do uso da amostra*Configurar uma política da inspeção de aplicativo HTTP para obstruir o 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
```

- **Inspeção do comprimento de campo de cabeçalho** — Este comando fornece uma capacidade para limitar o comprimento de uma linha de campo de cabeçalho. Reserve ou restaurar a ação pode ser aplicada a um pedido ou a uma resposta que combinam os critérios do mapa de classe. A adição da ação do log causa um mensagem do syslog:`APPFW-6- HTTP_HDR_FIELD_LENGTH.`*Comando usage:*`match {request|response|req-resp} header <header-name> length gt <bytes>` *Caso do uso da amostra*Configurar uma política do appfw HTTP para obstruir um pedido cujo o comprimento de campo do Cookie e do agente de usuário exceda o

256 e o 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
```

- Inspeção da repetição do campo de cabeçalho — Este comando verifica se um pedido ou uma resposta repetiram campos de cabeçalho. Reserve ou restaurar a ação pode ser aplicada a um pedido ou a uma resposta que combinam os critérios do mapa de classe. Quando permitida, a ação do log causa um mensagem do syslog:`APPFW-6-HTTP_REPEATED_HDR_FIELDS`.*Comando usage:*`match {request|response|req-resp} header <header-name>` *Caso do uso da amostra*Configurar uma política do appfw HTTP para obstruir um pedido ou uma resposta que tenha linhas de cabeçalho múltiplas do índice-comprimento. Esta é uma das funcionalidades as mais úteis usadas para impedir o contrabando da 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
```

- Inspeção do método — O HTTP RFC permite um grupo restrito de métodos HTTP. Contudo, mesmo alguns dos métodos padrão estão considerados inseguros enquanto alguns métodos podem ser usados para explorar vulnerabilidades em um servidor de Web. Muitos dos métodos não padronizados são usados frequentemente para a atividade mal-intencionada. Isto necessita uma necessidade de agrupar os métodos em várias categorias e de mandar o usuário escolher a ação para cada categoria. Este comando fornece o usuário uma maneira flexível de agrupar os métodos em várias categorias tais como métodos seguros, métodos inseguros, métodos do webdav, métodos RFC, e métodos prolongados. Reserve ou restaurar a ação pode ser aplicada a um pedido ou a uma resposta que combine os critérios do mapa de classe. A adição da ação do log causa um mensagem do syslog:`APPFW-6-HTTP_METHOD`.*Comando usage:*`match request method <method>` *Caso do uso da amostra*Configurar uma política do appfw HTTP que agrupe os métodos HTTP em três categorias: cofre forte, inseguro e webdav. Estes são mostrados na tabela. Configurar ações tais que:todos os métodos seguros são permitidos sem logtodos os métodos inseguros são permitidos com logtodos os métodos do webdav são obstruídos com log.`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
```

- **Inspeção URI** — Este comando fornece a capacidade para permitir/nega-os/pedidos do monitor cujo o URI combina a inspeção regular configurada. Isto dá ao usuário uma capacidade de obstruir o costume URL e as perguntas. Reserve ou restaurar a ação pode ser aplicada a um pedido ou a uma resposta que combinam os critérios do mapa de classe. A adição da ação do log causa um mensagem do syslog:`APPFW-6-HTTP_URI_REGEX_MATCHED` *Comando usage:* `match request uri regex <parameter-map-name>` *Caso do uso da amostra* Configurar uma política do appfw HTTP para obstruir um pedido cujo o URI combine qualqueras um 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 do comprimento URI** — Este comando verifica o comprimento do URI que está sendo enviado em um pedido e aplica a ação configurada quando o comprimento excede o limiar configurado. Reserve ou restaurar a ação pode ser aplicada a um pedido ou a uma resposta que combinam os critérios do mapa de classe. A adição da ação do log causa um mensagem do syslog:`APPFW-6- HTTP_URI_LENGTH.` *Comando usage:* `match request uri length gt <bytes>` *Caso do uso da amostra* Configurar uma política do appfw HTTP para levantar um alarme sempre que o comprimento URI de um pedido excede 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
```

- **Inspeção do argumento** — Este comando fornece uma capacidade para permitir, nega ou monitora o pedido cujos argumentos (parâmetros) combine a inspeção regular configurada. Reserve ou restaurar a ação pode ser aplicada a um pedido ou a uma resposta que combinam os critérios do mapa de classe. A adição da ação do log causa um mensagem do syslog:`APPFW-6- HTTP_ARG_REGEX_MATCHED` *Comando usage:* `match request arg regex <parameter-map-name>` *Caso do uso da amostra* Configurar uma política do appfw HTTP para obstruir um pedido cujos os argumentos combinem qualqueras um 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 do comprimento do argumento** — Este comando verifica o comprimento dos

argumentos que estão sendo enviados em um pedido e aplica a ação configurada quando o comprimento excede o limiar configurado. Reserve ou restaurar a ação pode ser aplicada a um pedido ou a uma resposta que combinam os critérios do mapa de classe. A adição da ação do log causa um mensagem do syslog:`APPFW-6- HTTP_ARG_LENGTH`.*Comando usage:*`match request arg length gt <bytes>` *Caso do uso da amostra*Configurar uma política do appfw HTTP para levantar um alarme sempre que o comprimento do argumento de um pedido excede 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
```

- Inspeção de corpo — Este CLI permite que o usuário especifique a lista de expressões regulares a ser combinadas contra o corpo do pedido ou da resposta. Reserve ou restaurar a ação pode ser aplicada a um pedido ou a uma resposta que combinam os critérios do mapa de classe. A adição da ação do log causa um mensagem do syslog:`APPFW-6-HTTP_BODY_REGEX_MATCHED`*Comando usage:*`match {request|response|reg-resp} body regex <parameter-map-name>` *Caso do uso da amostra*Configurar um appfw HTTP para obstruir uma resposta cujo o corpo contenha o teste padrão. `* [Kk] do [Cc] do [Aa] do [Tt] do [Tt] do [Aa]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 (satisfeita) do comprimento do corpo — Este comando verifica o tamanho da mensagem que está sendo enviada com o pedido ou a resposta. Reserve ou restaurar a ação pode ser aplicada a um pedido ou a uma resposta que combinam os critérios do mapa de classe. A adição da ação do log causa um mensagem do syslog:`APPFW-4-HTTP_CONTENT_LENGTH`*Comando usage:*`match {request|response|req-resp} body length lt <bytes> gt <bytes>` *Caso do uso da amostra*Configurar uma política do appfw HTTP para obstruir uma sessão de HTTP que leve mais então a mensagem dos bytes 10K em um pedido ou em uma 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
```

- Inspeção da linha de status — O comando permite que o usuário especifique a lista de expressões regulares a ser combinadas contra a linha de status de uma resposta. Reserve ou restaurar a ação pode ser aplicada a um pedido ou a uma resposta que combinam os critérios do mapa de classe. A adição da ação do log causa um mensagem do syslog:`APPFW-6-HTTP_STLINE_REGEX_MATCHED`.*Comando usage:*`match response status-line regex <class-map-name>` *Caso do uso da amostra*Configurar um appfw HTTP para registrar um alarme sempre que uma tentativa é feita para alcançar uma página proibida. Uma página proibida contém geralmente um código de status 403 e a linha de status olha como a `página HTTP/1.0 403 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
```

- **Inspeção do tipo de conteúdo** — Este comando verifica se o tipo de conteúdo do cabeçalho da mensagem está na lista dos tipos de conteúdo apoiados. Igualmente verifica que o tipo de conteúdo do encabeçamento combina o índice da parcela dos dados de mensagem ou do corpo de entidade. Se a **má combinação da** palavra-chave é configurada, o comando verifica o tipo de conteúdo do mensagem de resposta contra o valor de campo aceitado do mensagem request. Reserve ou restaurar a ação pode ser aplicada a um pedido ou a uma resposta que combinam os critérios do mapa de classe. A adição da ação do log causa o mensagem do syslog apropriado:`APPFW-4- HTTP_CONT_TYPE_VIOLATION, APPFW-4- HTTP_CONT_TYPE_MISMATCH, APPFW-4- HTTP_CONT_TYPE_UNKNOWN`*Comando usage:*`match {request|response|req-resp} header content-type [mismatch|unknown|violation]`*Caso do uso da amostra*Configurar uma política do appfw HTTP para obstruir uma sessão de HTTP que leve os pedidos e as respostas que têm 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 do Porta-emprego errado** — Este comando é usado impedir a porta HTTP (80) que está sendo empregada mal para outros aplicativos tais como IM, P2P, Tunelamento, etc. reservam ou restaurar a ação pode ser aplicada a um pedido ou a uma resposta que combinam os critérios do mapa de classe. A adição da ação do log causa o mensagem do syslog apropriado:`APPFW-4- HTTP_PORT_MISUSE_TYPE_IM APPFW-4-HTTP_PORT_MISUSE_TYPE_P2P APPFW-4-HTTP_PORT_MISUSE_TYPE_TUNNEL`*Comando usage:*`match request port-misuse {im|p2p|tunneling|any}`*Caso do uso da amostra*Configurar uma política do appfw HTTP para obstruir uma sessão de HTTP que está sendo empregada mal para IM o aplicativo.
```
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
```

- **inspeção Restrito-HTTP** — Este comando permite a verificação restrita da conformidade do protocolo contra pedidos do HTTP e respostas. Reserve ou restaurar a ação pode ser aplicada a um pedido ou a uma resposta que combinam os critérios do mapa de classe. A adição da ação do log causa um mensagem do syslog:`APPFW-4- HTTP_PROTOCOL_VIOLATION`*Comando usage:*`match req-resp protocol-violation`*Caso do uso da amostra*Configurar uma política do appfw HTTP para obstruir os pedidos ou as respostas que violam 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 da Transferência-codificação** — Este comando fornece uma capacidade para permitir, nega ou monitora o pedido/resposta cujo o tipo da codificação de transferência combina com o tipo configurado. Reserve ou restaurar a ação pode ser aplicada a um pedido ou a uma resposta que combinam os critérios do mapa de classe. A adição da ação do log

causa um mensagem do syslog:`APPFW-6- HTTP_TRANSFER_ENCODING`*Comando usage:*`match {request|response|req-resp} header transfer-encoding {regex <parameter-map-name> |gzip|deflate|chunked|identity|all}` *Caso do uso da amostra*Configurar uma política do appfw HTTP para obstruir um pedido ou uma resposta que tenha o tipo codificação da compressa.

```
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
```

- Inspeção do Java applet — Este comando verifica se uma resposta tem o Java applet e aplica a ação configurada após detecção do applet. Reserve ou restaurar a ação pode ser aplicada a um pedido ou a uma resposta que combinam os critérios do mapa de classe. A adição da ação do log causa um mensagem do syslog:`APPFW-4- HTTP_JAVA_APPLET` *Comando usage:*`match response body java-applet`*Caso do uso da amostra*Configurar uma política do appfw HTTP para obstruir Java applets.

```
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
```

Apoio ZFW para mensagens instantâneas e o controle de aplicativo peer-to-peer

O Cisco IOS Software Release 12.4(9)T introduziu o apoio ZFW para aplicativos de IM e P2P.

O Cisco IOS Software ofereceu primeiramente o apoio para IM o controle de aplicativo no Cisco IOS Software Release 12.4(4)T. A versão inicial de ZFW não fez aplicativo do apoio IM na relação ZFW. Se o controle de aplicativo IM foi desejado, os usuários eram incapazes de migrar à interface de configuração ZFW. O Cisco IOS Software Release 12.4(9)T introduz o apoio ZFW para IM a inspeção, apoiando Yahoo! Mensageiro (YM), MSN Messenger (MSN), e AOL Instant Messenger (AIM).

O Cisco IOS Software Release 12.4(9)T é a primeira versão de Cisco IOS Software que oferece o apoio do Firewall do Native IOS para aplicativos de compartilhamento de arquivos P2P.

Políticas da camada 4 e da camada 7 da oferta de amba a inspeção de IM e P2P para o tráfego de aplicativo. Isto significa que ZFW pode fornecer a inspeção stateful básica para permitir o permit or deny o tráfego, assim como o controle granulado da camada 7 em atividades específicas nos vários protocolos, de modo que determinadas atividades do aplicativo sejam permitidas quando outro forem negadas.

Inspeção de aplicativo e controle P2P

O SDM 2.2 introduziu o controle de aplicativo P2P em sua seção de configuração de firewall. O SDM aplicou um Network-Based Application Recognition (NBAR) e uma política de QoS para detectar e uma atividade do aplicativo P2P da polícia a uma linha taxa de zero, obstruindo todo o tráfego P2P. Isto levantou a edição que os usuários CLI, esperando o apoio P2P no firewall de IOS CLI, eram incapazes de configurar o P2P que obstrui no CLI a menos que estivessem cientes da configuração necessária NBAR/QoS. O Cisco IOS Software Release 12.4(9)T introduz o controle nativo P2P no ZFW CLI, leveraging o NBAR para detectar a atividade do aplicativo P2P. Este suportes para o software release diversos protocolos do aplicativo P2P:

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

Os aplicativos P2P são particularmente difíceis de detectar, em consequência do comportamento da “porta-lupulagem” e dos outros truques para evitar a detecção, assim como dos problemas introduzidos por mudanças e por atualizações frequentes aos aplicativos P2P que alteram os comportamentos dos protocolos. ZFW combina a inspeção stateful nativa do Firewall com as capacidades do tráfego-reconhecimento do NBAR de entregar o controle de aplicativo P2P na interface de configuração COMPLETA de ZFW. O NBAR oferece dois benefícios excelentes:

- O reconhecimento de aplicativo heurístico-baseado opcional para reconhecer aplicativos apesar do complexo, difícil-à-detecta o comportamento
- Infraestrutura elástico que oferece um mecanismo da atualização ficar lado a lado das atualizações de protocolo e das alterações

Configurando a inspeção P2P

Como mencionado mais cedo, a inspeção P2P e o controle oferecem a inspeção stateful da camada 4 e o controle de aplicativo da camada 7.

A inspeção da camada 4 é configurada similarmente a outros serviços de aplicativo, se a inspeção das portas nativas dos serviços de aplicativo será 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 adicional da assinatura no [service-name] do protocolo do fósforo. Adicionando a opção da assinatura no fim da declaração de protocolo do fósforo, as heurísticas NBAR são aplicadas ao tráfego para procurar pelos telltales no tráfego que indicam a atividade específica do aplicativo P2P. Isto inclui a porta-lupulagem e as outras mudanças no comportamento de aplicativo para evitar a detecção do tráfego. Este nível da inspeção do tráfego vem a preço da utilização CPU aumentada e da capacidade reduzida do throughput de rede. Se a opção da assinatura não é análise heurística aplicada, NBAR-baseada não estará aplicado para detectar o comportamento da porta-lupulagem, e a utilização CPU não será impactada à mesma extensão.

A inspeção de serviço nativa leva a desvantagem que é incapaz de manter o controle sobre aplicativos P2P caso o aplicativo “saltos” a uma porta de origem e de destino não padronizada, ou se o aplicativo é atualizado começar sua ação em um número de porta não reconhecido:

Aplicativo	Portas nativas (como reconhecido pela lista 12.4(15)T PAM)
bittorrent	TCP 6881-6889
edonkey	TCP 4662
fasttrack	TCP 1214

gnutella	TCP 6346-6349 TCP 6355,5634 UDP 6346-6348
kazaa2	Dependente no PAM
winmx	TCP 6699

Se você deseja permitir (para inspecionar) o tráfego P2P, você pôde precisar de fornecer a configuração adicional. Alguns aplicativos puderam usar redes múltiplas P2P, ou execute os comportamentos específicos que você pôde precisar de acomodar em sua configuração de firewall para permitir o aplicativo trabalhar:

- Os clientes de BitTorrent comunicam-se geralmente com os “perseguidores” (servidores de diretório do par) através do HTTP que é executado em alguma porta não padronizada. Este é tipicamente TCP 6969, mas você pôde precisar de verificar a porta torrente-específica do perseguidor. Se você deseja permitir BitTorrent, o melhor método para acomodar a porta adicional é configurar o HTTP como um dos protocolos do fósforo e adicionar TCP 6969 ao HTTP usando o **comando ip port-map**:
  `ip port-map http port tcp 6969` Você precisará de definir o HTTP e bittorrent como os critérios de verificação de repetição de dados aplicados no mapa de classe.
- o eDonkey parece iniciar as conexões que são detectadas como o eDonkey e o Gnutella.
- A inspeção de KaZaA é inteiramente dependente da detecção da NBAR-assinatura.

Mergulhe (aplicativo) a inspeção 7 aumenta a inspeção da camada 4 com a capacidade de reconhecer e aplicar ações das específicas do serviço, tais como seletivamente a obstrução ou permitir da arquivo-busca, da transferência de arquivo, e das capacidades do texto-bate-papo. As capacidades das específicas do serviço variam pelo serviço.

A inspeção de aplicativo P2P é similar à inspeção de aplicativo 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 aplicativo P2P oferece capacidades características da aplicação para um subconjunto dos aplicativos apoiados pela inspeção da camada 4:

- edonkey
- fasttrack
- gnutella

- kazaa2

Cada um destas ofertas dos aplicativos que variam critérios de verificação de repetição de dados característicos da aplicação das opções:

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)#match ? file-transfer Match file transfer stream flow Flow based QoS parameters
```

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
```

As definições ou as atualizações novas do protocolo P2P aos protocolos existentes P2P podem ser carregadas usando a funcionalidade dinâmica da atualização do pdlm do NBAR. Este é o comando configuration carregar o PDLM novo:

ip nbar pdlm *<file-location>*

O protocolo novo está disponível em comandos do protocolo do fósforo… para a classe que o tipo inspeciona. Se o protocolo novo P2P tem serviços (secundário-protocolos), a camada nova 7 inspeciona tipos do mapa de classe, assim como os critérios de verificação de repetição de dados da camada 7, tornam-se disponíveis.

IM inspeção de aplicativo e controle

O Cisco IOS Software Release 12.4(4)T introduziu a inspeção de aplicativo IM e o controle. O apoio IM não foi introduzido com o ZFW em 12.4(6)T, assim que os usuários eram incapazes de aplicar o controle IM e o ZFW na mesma política de firewall, porque os recursos de firewall ZFW e de legado não podem coexistir em uma dada interface.

O Cisco IOS Software Release 12.4(9)T apoia a inspeção stateful e o controle de aplicativo para estes serviços IM:

- AOL Instant Messenger
- MSN Messenger
- Yahoo! Mensageiro

A inspeção IM varia levemente da maioria de serviços, porque a inspeção IM confia no acesso de controlo a um grupo específico de anfitriões para cada dado serviço. Os serviços IM confiam geralmente em um grupo relativamente permanente de servidores de diretório, que os clientes devem poder contactar a fim alcançar o serviço IM. Os aplicativos IM tendem a ser muito difíceis de controlar de um ponto de vista do protocolo ou do serviço. A maioria de maneira eficaz controlar estes aplicativos é limitar o acesso aos server IM fixos.

Configurando a inspeção IM

A inspeção IM e o controle oferecem a inspeção stateful da camada 4 e o controle de aplicativo da camada 7.

A inspeção da camada 4 é configurada similarmente a outros serviços de aplicativo:

```
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
```

Os aplicativos IM podem contactar seus server em portas múltiplas para manter sua funcionalidade. Se você deseja permitir um serviço IM dado aplicando a ação da inspeção, você não pôde precisar uma lista de servidor de definir o acesso permitido aos server do serviço IM. Contudo, configurar um mapa de classe que especifica um serviço IM dado, tal como AOL Instant Messenger, e a aplicação da ação de queda no mapa de política associado pode fazer com que o cliente IM tente e encontre uma porta diferente onde a Conectividade seja permitida ao Internet. Se você não quer permitir a Conectividade a um dado serviço, ou se você quer restringir o texto-bate-papo da capacidade de serviço IM, você deve definir uma lista de servidor assim que o ZFW pode identificar o tráfego associado com o aplicativo 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 Yahoo IM é definida como esta'n:

```
parameter-map type protocol-info ymsgr-pmap
  server name scs.msg.yahoo.com
  server name scsd.msg.yahoo.com
  server ip 66.77.88.99
  server ip range 103.24.5.67 103.24.5.99
```

Você precisará de aplicar a lista de servidor à definição do protocolo:

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

Você deve configurar a **consulta de domínio IP** e os comandos de **ip.ad.re.ss do Nome do servidor IP** a fim permitir a resolução de nome.

Os nomes do servidor IM são razoavelmente dinâmicos. Você precisará de certificar-se de periodicamente suas listas de servidor IM configuradas estejam completas e corretas.

Mergulhe (aplicativo) a inspeção 7 aumenta a inspeção da camada 4 com a capacidade de reconhecer e aplicar ações das específicas do serviço, tais como seletivamente a obstrução ou permitir de capacidades do texto-bate-papo, ao negar capacidades de outro serviço.

IM a inspeção de aplicativo oferece presentemente a capacidade de diferenciar-se entre a atividade do texto-bate-papo e os todos serviços de aplicativo restantes. A fim restringir o texto-bate-papo da atividade IM, configurar uma política da 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 a Yahoo! Política do mensageiro configurada mais cedo:

```
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
```

Filtragem URL

ZFW oferece capacidades da Filtragem URL de limitar o acesso ao conteúdo da Web àquela especificado por um branco ou por uma lista negra definido no roteador, ou enviando Domain Name a um server da Filtragem URL para verificar o acesso aos domínios específicos. A Filtragem URL ZFW nos Cisco IOS Software Release 12.4(6)T a 12.4(15)T é aplicada como uma ação de política adicional, similar à inspeção de aplicativo.

Para a Filtragem URL server-baseada, você deve definir um parâmetro-mapa que descreva a configuração do servidor do **urlfilter**:

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

Se brancos estáticos ou as listas negras são preferidos, você pode definir uma lista de domínios ou de subdomínios que especificamente estão permitidos ou negados, quando a ação inversa for aplicada para traficar que não combina a lista:

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

Se uma lista negra URL é utilização definida negue opções nas definições do exclusivo-domínio, todos domínios restantes estará reservado. Se alguma definição da “licença” é definida, todos os domínios que serão permitidos devem explicitamente ser especificados, similar à função de listas de controle de acesso IP.

Estabelecer um mapa de classe que combine o tráfego de HTTP:

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

Defina um mapa de política que associa seu mapa de classe com **inspecionam** e ações do **urlfilter**:

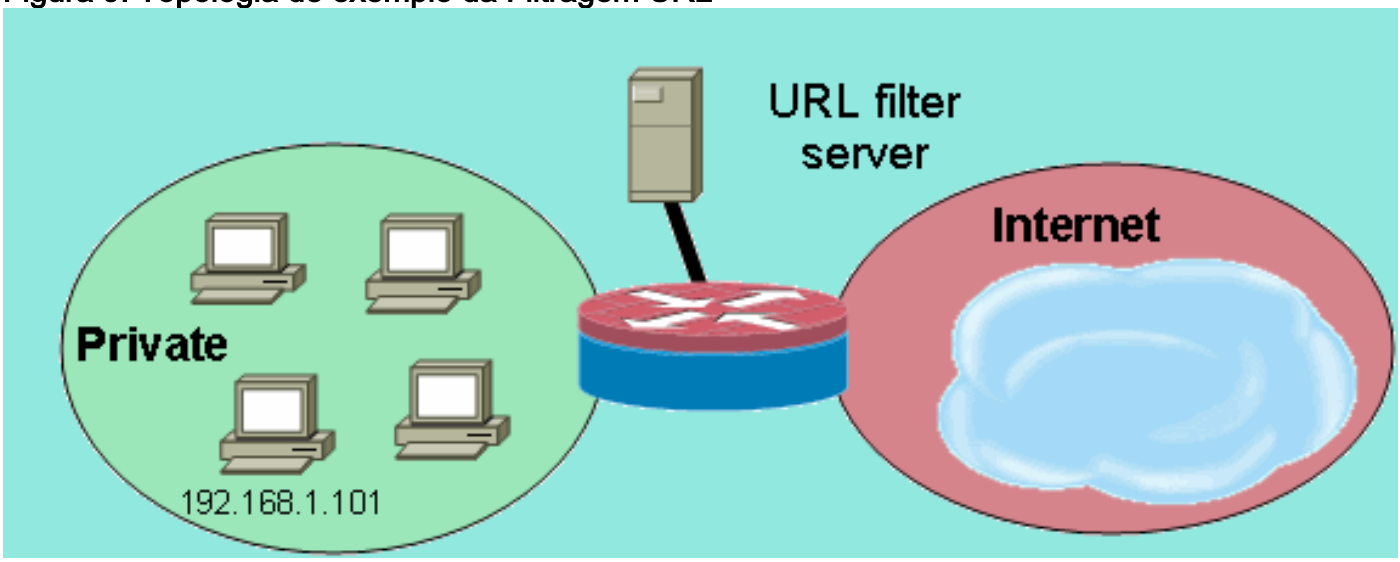
```
policy-map type inspect http-filter-pmap
 class type inspect http-cmap
  inspect
  urlfilter websense-parmap
```

Isto configura o requisito mínimo para comunicar-se com um server da Filtragem URL. Diversas opções estão disponíveis para definir o comportamento adicional da Filtragem URL.

Algumas distribuições de rede puderam querer aplicar a Filtragem URL para algumas anfitriões

ou sub-redes, ao contornear a Filtragem URL para outros anfitriões. Por exemplo, na figura 9, todos os anfitriões na zona privada devem ter o tráfego de HTTP verificado por um server do filtro URL, à exceção do host específico 192.168.1.101.

Figura 9: Topologia de exemplo da Filtragem URL



Isto pode ser realizado definindo dois mapas diferentes do mapa de classe:

- Um mapa de classe que combina somente o tráfego de HTTP para o grupo maior de anfitriões, que receberão a Filtragem URL.
- Um mapa de classe para o grupo menor de anfitriões, que não receberão a Filtragem URL. O segundo mapa de classe combinará o tráfego de HTTP, assim como uma lista de anfitriões que serão isentados da política da Filtragem URL.

Ambos os mapas de classe são configurados em um mapa de política, mas somente um receberá a ação do **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
```

Acesso de controlo ao roteador

A maioria de coordenadores da segurança de rede são incômodos expondo as interfaces de gerenciamento do roteador (por exemplo, SSH, telnet, HTTP, HTTPS, SNMP, e assim por diante) aos Internet públicas, e em certas circunstâncias, o controle pôde ser precisado para o acesso de LAN ao roteador também. O Cisco IOS Software oferece um número de opções limitar o acesso às várias relações, que inclui a família da característica da proteção da fundação da rede (NFP), vários mecanismos do controle de acesso para interfaces de gerenciamento, e auto-zona de ZFW. Você deve rever outros recursos, tais como o controle de acesso VTY, a proteção do plano de gerenciamento, e o controle de acesso SNMP para determinar que combinação de

características do controle do roteador trabalhará melhor para seu aplicativo específico.

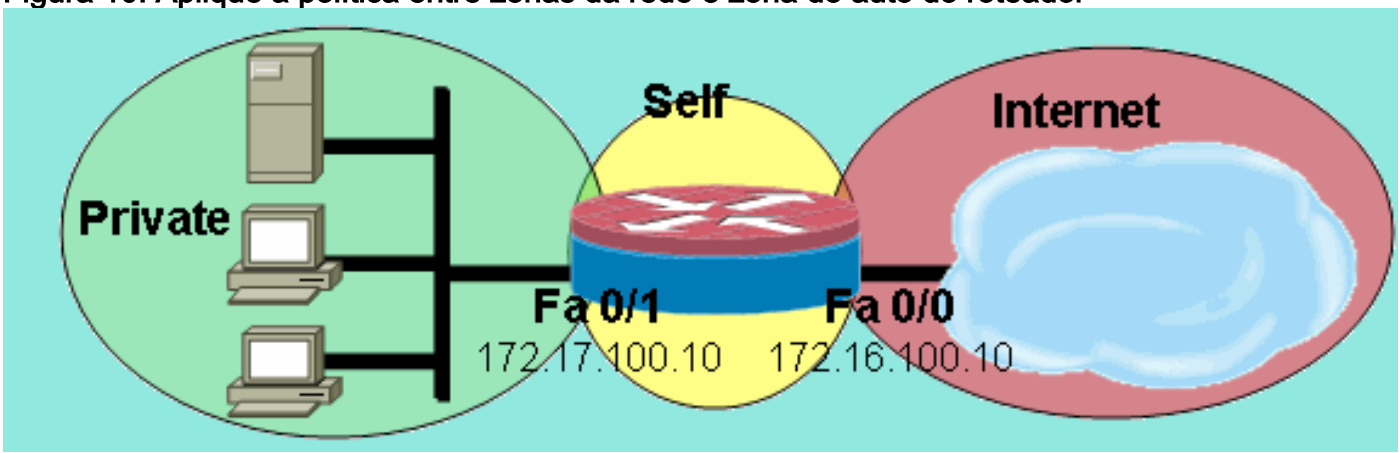
Geralmente, a família da característica NFP é serida melhor para o controle do tráfego destinado para o roteador próprio. Refira a Visão Geral de Segurança do plano do controle no Cisco IOS Software para a informação que descreve a proteção do roteador usando as características NFP.

Se você decide aplicar ZFW ao tráfego de controle a e dos endereços IP de Um ou Mais Servidores Cisco ICM NT no roteador próprio, você deve compreender que a política padrão e as capacidades do Firewall diferem daquelas disponíveis para o tráfego de trânsito. O tráfego de trânsito é definido como o tráfego de rede cujos os endereços IP de origem e de destino não combinam nenhuns endereços IP de Um ou Mais Servidores Cisco ICM NT aplicada a algumas das relações do Roteadores, e o tráfego não fará com que o roteador enviem, por exemplo, as mensagens do controle de rede tais como a expiração ICMP TTL ou a rede/mensagens do host inalcançável.

ZFW aplica um padrão negar-toda política para traficar mover-se entre zonas, exceto, como mencionado nas regras gerais, tráfego em toda a zona que flui diretamente aos endereços das relações do roteador é reservado implicitamente. Isto assegura que a Conectividade às interfaces de gerenciamento do roteador está mantida quando uma configuração de firewall da zona é aplicada ao roteador. Se mesma negar-toda política afetou a Conectividade diretamente ao roteador, uma configuração completa da política de gerenciamento teria que ser aplicada antes que as zonas estejam configuradas no roteador. Isto interromperia provavelmente a Conectividade do Gerenciamento se a política impropriamente foi executada ou aplicada na ordem errada.

Quando uma relação é configurada para ser um membro da zona, os anfitriões conectados à relação estão incluídos na zona. Contudo, o fluxo de tráfego a e dos endereços IP de Um ou Mais Servidores Cisco ICM NT das relações do roteador não é controlado pelas políticas da zona (à excecpção das circunstâncias descritas na nota depois da figura 10). Em lugar de, todas as interfaces IP no roteador estão feitas automaticamente parte de à zona do auto quando ZFW é configurado. A fim controlar o tráfego IP que move-se para as relações do roteador das várias zonas em um roteador, as políticas devem ser aplicadas para obstruir ou para reservar/inspecione o tráfego entre a zona e a zona do auto do roteador, e vice-versa. (Veja figura 10.)

Figura 10: Aplique a política entre zonas da rede e zona do auto do roteador



Embora o roteador ofereça uma política da padrão-permissão entre todas as zonas e a zona do auto, se uma política está configurada de qualquer zona à zona do auto, e nenhuma política está configurada do auto às zonas relação-conectadas configuráveis pelo usuário do roteador, todo o tráfego roteador-originado encontra a política da auto-zona da conectar-zona em seu retorno o roteador e está obstruído. Assim, o tráfego roteador-originado deve ser inspecionado para permitir

seu retorno à zona do auto.

Nota: O Cisco IOS Software usa sempre o endereço IP de Um ou Mais Servidores Cisco ICM NT associado com os host de destino “os mais próximos” de uma relação para o tráfego tal como o Syslog, o tftp, o telnet, e os outros serviços do controle plano, e sujeita esta política de firewall da auto-zona do tráfego. Contudo, se um serviço define uma relação específica como a interface de origem usando os comandos que incluem, mas não limitado ao **[type number] de registro da interface de origem**, ao **[type number] da interface de origem IP tftp**, e ao **[type number] da interface de origem do telnet IP**, o tráfego é sujeitado à auto-zona.

Nota: Alguns serviços (particularmente serviços Voz-sobre-IP do Roteadores) usam as relações efêmeras ou não-configurável que não podem ser atribuídas às zonas de Segurança. Estes serviços não puderam funcionar corretamente se seu tráfego não pode ser associado com uma zona de Segurança configurada.

Limitações da política da Auto-zona

a política da Auto-zona limitou a funcionalidade em relação às políticas disponíveis para zona-pares do tráfego de trânsito:

- Como era o caso com inspeção stateful clássica, o tráfego roteador-gerado é limitado ao TCP, ao UDP, ao ICMP, e à inspeção do protocolo complexo para H.323.
- A inspeção de aplicativo não está disponível para políticas da auto-zona.
- A sessão e avalia a limitação não pode ser configurada em políticas da auto-zona.

Configuração das normas da Auto-zona

Sob a maioria de circunstâncias, estas são políticas de acesso desejáveis para serviços de gernciamento de roteador:

- Negue toda a conectividade telnet, como o protocolo da minuta do telnet expõe facilmente credenciais do usuário e a outra informação sensível.
- Permita conexões de SSH de todo o usuário em qualquer zona. O SSH cifra credenciais do usuário e dados de sessão, que fornecem a proteção dos usuários maliciosos que empregam a pacote-captura de ferramentas à espião em credenciais ou em informação sensível do usuário da atividade e do acordo do usuário tal como a configuração de roteador. A versão de SSH 2 fornece uma proteção mais forte, e as vulnerabilidades específicas dos endereços inerentes à versão de SSH 1.
- Permita a Conectividade HTTP ao roteador das zonas privadas, se a zona privada é de confiança. Se não, se a zona privada abriga o potencial para que os usuários maliciosos comprometam a informação, o HTTP não emprega a criptografia para proteger o tráfego de gerenciamento, e pôde revelar a informação sensível tal como credenciais ou configuração do usuário.
- Permita a Conectividade HTTPS de toda a zona. Similar ao SSH, o HTTPS cifra dados de sessão e credenciais do usuário.
- Restrinja o acesso SNMP a um host ou a uma sub-rede específica. O SNMP pode ser usado para alterar a configuração de roteador e revelar a informação de configuração. O SNMP deve ser configurado com controle de acesso nas várias comunidades.
- Pedidos do bloco ICMP dos Internet públicas ao endereço da privado-zona (supor o endereço

da privado-zona é roteável). Uns ou vários endereços públicos podem ser expostos para o tráfego ICMP para o Troubleshooting da rede, caso necessário. Diversos ataques ICMP podem ser usados para oprimir recursos de roteador ou fazer reconhecimento de terreno a topologia de rede e a arquitetura.

Um roteador pode aplicar este tipo de política com a adição de dois zona-pares para cada zona que deve ser controlada. Cada zona-par para o tráfego de entrada, ou de partida, da auto-zona do roteador deve ser combinado pela política respectiva na direção oposta, a menos que o tráfego não for originado na direção oposta. Um mapa de política cada um para zona-pares de entrada e de partida pode ser aplicado que descreve todo o tráfego, ou os política-mapas específicos por zona-pares podem ser aplicados. A configuração de zona-pares específicos pelo mapa de política fornece a granularidade para a atividade de vista que combina cada mapa de política.

Supondo uma rede de exemplo com uma estação do gerenciamento de SNMP em 172.17.100.11, e um servidor TFTP em 172.17.100.17, esta saída fornece um exemplo da política de acesso inteira 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 da auto-zona não oferece a capacidade de inspecionar transferências de TFTP. Assim, o Firewall deve passar todo o tráfego a e do servidor TFTP se o TFTP deve passar com o Firewall.

Se o roteador terminará conexões do IPSec VPN, você deve igualmente definir uma política para passar o IPsec ESP, o IPsec AH, o IPsec ISAKMP, e NAT-T (UDP 4500). Isto depende de qual é precisado com base lhe presta serviços de manutenção se usará. A seguinte política pode ser aplicada além do que a política acima. Note a mudança aos política-mapas onde um mapa de classe para o tráfego VPN foi introduzido com uma ação da passagem. Tipicamente, o tráfego criptografado é de confiança, a menos que sua política de segurança indicar que você deve permitir o tráfego criptografado a e dos valores-limite 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
```

Firewall e Wide Area Application Services Zona-baseados

Refira o Release Note para novos recursos do Wide Area Application Services de Cisco (versão de software 4.0.13) - para a versão de software 4.0.13 para uma nota do aplicativo que forneça exemplos de configuração e orientação do uso

Monitorando o Firewall Zona-baseado da política com comandos show and debug

ZFW introduz comandos new a fim ver a configuração das normas e monitorar a atividade do Firewall.

Indique a descrição da zona e as relações contidas em uma zona especificada:

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

Quando o nome de zona não é incluído, o comando indica a informação de todas as zonas configuradas.

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

Indique a zona de origem, a zona de destino e a política anexadas aos zona-pares:

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

Quando nenhum fonte ou destino são especificados, todos os zona-pares com fonte, destino, e a política associada estão indicados. Quando somente a fonte/zona de destino for mencionada, todos os zona-pares que contêm esta zona enquanto a fonte/destino é indicada.

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

Indica um mapa de política especificado:

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

Quando o nome de um mapa de política não é especificado, indica todos os política-mapas do tipo inspeciona (incluindo os política-mapas da camada 7 que contêm um subtipo).

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

Indica o tempo de execução inspecionam o tipo estatísticas do mapa de política que existem em um zona-par especificado.

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

Quando **nenhum nome dos zona-pares** é mencionado, os política-mapas em todos os zona-pares estão indicados.

A opção das **sessões** indica as sessões da inspeção criadas pelo aplicativo do mapa de política nos zona-pares especificados.

```
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 do **urlfilter** indica as estatísticas urlfilter-relacionadas que se referem o mapa de política especificado (ou política-mapas em todos os alvos quando nenhum nome dos zona-pares é especificado):

show policy-map type inspect zone-pair [*zone-pair-name*] [urlfilter [cache]]
Quando a palavra-chave do **esconderijo** é especificada junto com o **urlfilter**, indica o esconderijo do **urlfilter** (dos endereços IP de Um ou Mais Servidores Cisco ICM NT).

O sumário do **comando show policy-map** para inspeciona política-mapas:

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

Proteção Zona-baseada de ajustamento da recusa de serviço do Firewall da política

ZFW oferece a proteção de DOS alertar engenheiros de rede às mudanças dramáticas na atividade de rede, e abrandar atividade indesejável para reduzir o impacto de mudanças da atividade de rede. ZFW mantém um contador separado para cada mapa de classe dos política-mapas. Assim, se um mapa de classe é usado para os dois política-mapas dos zona-pares diferentes, dois grupos diferentes de contadores da proteção de DOS serão aplicados.

ZFW fornece a mitigação do ataque DoS como um padrão em Cisco IOS Software Release antes de 12.4(11)T. O comportamento da proteção de DOS do padrão mudado com Cisco IOS Software Release 12.4(11)T. Refira a proteção de ajustamento da recusa de serviço do Cisco IOS Firewall para que uma discussão mais adicional e um procedimento ajuste a proteção de DOS ZFW.

Refira a definição de estratégias para proteger contra o ataque de recusa de serviço TCP SYN para obter mais informações sobre dos ataques DoS TCP SYN.

Apêndice

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 (completa) final

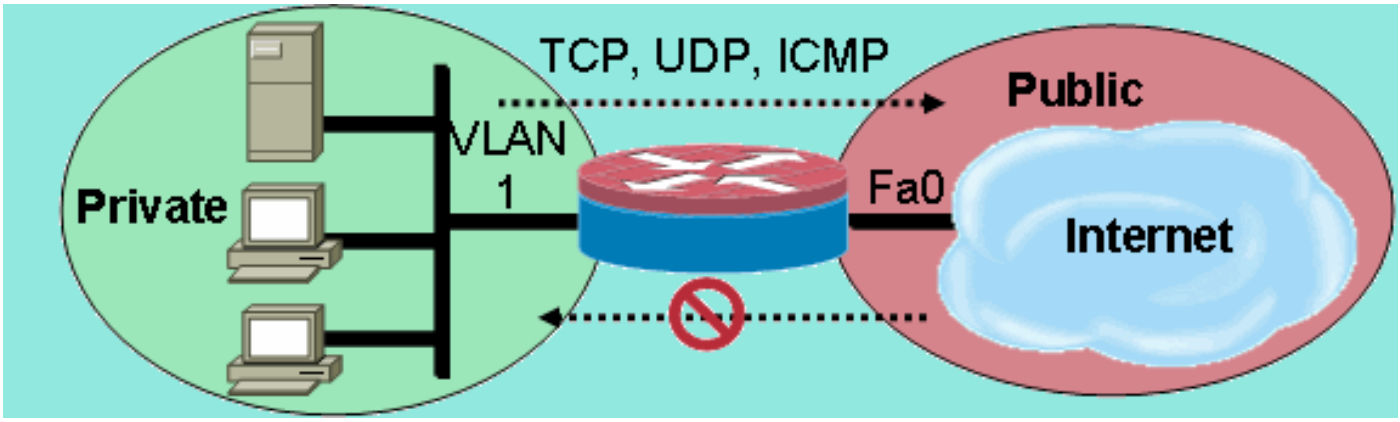
```
ip subnet-zero
ip cef
!
ip port-map user-Xwindows port tcp from 6900 to 6910
!
class-map type inspect match-any L4-inspect-class
 match protocol tcp
 match protocol udp
 match protocol icmp
class-map type inspect match-any L7-inspect-class
  match protocol ssh
  match protocol ftp
  match protocol 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 de firewall básica da Zona-política para duas zonas

Este exemplo fornece uma configuração simples como base para testes da característica para realces ao Cisco IOS Software ZFW. Esta configuração é uma configuração modelo para duas zonas, como configurado em um 1811 Router. A zona privada é aplicada às portas do switch fixo do roteador, assim que todos os anfitriões nas portas de switch são conectados ao VLAN1. A zona pública é aplicada nos 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