瞭解基於區域的策略防火牆設計

目錄

簡介

本檔案介紹Cisco IOS®防火牆功能集(基於區域的策略防火牆(ZFW))的配置模型。

必要條件

需求

本文件沒有特定需求。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

背景資訊

此新配置模型為多介面路由器提供了直觀的策略，提高了防火牆策略應用的粒度，並提供了預設的deny-all策略，該策略在應用顯式策略以允許所需流量之前禁止防火牆安全區域之間的流量。

基於區域的新策略檢測介面支援在Cisco IOS軟體版本12.4(6)T之前實施的幾乎所有傳統Cisco IOS防火牆功能：

- 狀態封包檢測
- VRF感知Cisco IOS防火牆
- URL篩選

- 阻斷服務(DoS)緩解

Cisco IOS軟體版本12.4(9)T新增了對每類作業階段/連線和輸送量限制以及應用程式檢查和控制的ZFW支援：

- HTTP
- 郵局通訊協定(POP3)、網際網路郵件存取通訊協定(IMAP)、簡易郵件傳輸通訊協定/增強型簡易郵件傳輸通訊協定(SMTP/ESMTP)
- Sun遠端程式呼叫(RPC)
- 即時消息(IM)應用程式：Microsoft Messenger雅虎！MessengerAOL即時通訊工具
- 對等(P2P)檔案共用：BittorrentKaZaA格努特拉驢子

Cisco IOS軟體版本12.4(11)T新增了統計資料，可更輕鬆地DoS保護調整。

Cisco IOS軟體版本12.4(15)T中的ZFW尚支援某些Cisco IOS經典防火牆功能和功能：

- 驗證代理
- 狀態防火牆故障切換
- 整合防火牆MIB
- IPv6狀態檢測
- TCP無序支援

對於大多數防火牆檢查活動，ZFW一般會提高Cisco IOS效能。Cisco IOS ZFW和Classic Firewall都不包含對組播流量的狀態檢測支援。

基於區域的策略概述

Cisco IOS傳統防火牆狀態檢測（以前稱為基於情景的訪問控制，或CBAC）採用了基於介面的配置模型，其中狀態檢測策略應用於介面。通過該介面的所有流量都收到了相同的檢查策略。此配置模型限制了防火牆策略的粒度，並造成防火牆策略正確應用的混亂，尤其是在必須在多個介面之間應用防火牆策略的情況下。

基於區域的策略防火牆（也稱為區域策略防火牆，或ZFW）將防火牆配置從較舊的基於介面的模型更改為更靈活、更易於理解的基於區域的模型。介面分配給區域，檢查策略應用於在區域之間移動的流量。區域間策略提供了相當大的靈活性和精細度，因此可以將不同的檢查策略應用於連線到同一路由器介面的多個主機組。

防火牆策略使用思科策略語言(CPL)進行配置，該語言採用分層結構來定義對網路協定和可應用檢查的主機組的檢查。

基於區域的策略配置模型

與Cisco IOS經典防火牆相比，ZFW完全改變了配置Cisco IOS防火牆檢測的方式。

對防火牆配置的第一個主要更改是引入了基於區域的配置。Cisco IOS防火牆是首個實施區域配置模型的Cisco IOS軟體威脅防禦功能。隨著時間的推移，其它特徵可以採用區域模型。使用ip inspect命令集的Cisco IOS傳統防火牆狀態檢查（或CBAC）基於介面的配置模型會保留一段時間。然而，很少有新功能（如果有的話）可以通過傳統的命令列介面(CLI)配置。ZFW不使用狀態檢測或CBAC命令。這兩種配置模型可在路由器上同時使用，但不能結合在介面上。介面不能配置為安全區域成員，同時配置為ip inspect。

區域建立網路的安全邊界。區域定義一個邊界，在該邊界中，流量在穿過網路的其他區域時會受到

策略限制。區域之間的ZFW預設策略為deny all。如果沒有明確配置策略，則會阻止在區域之間移動的所有流量。這明顯偏離了狀態檢查模式，在該模式中，流量被隱式允許直到被訪問控制清單(ACL)顯式阻止。

第二個主要變化是引入了一種新的配置策略語言CPL。熟悉Cisco IOS軟體模組化服務品質(QoS)CLI(MQC)的使用者可識別出此格式類似於QoS使用類別對映來指定哪些流量受策略對映中應用的操作影響。

基於區域的策略防火牆應用的規則

區域中的路由器網路介面成員資格受若幹管理介面行為的規則的約束，區域成員介面之間移動的流量也是如此：

- 必須先配置區域，然後才能將介面分配給區域。
- 一個介面只能分配給一個安全區域。
- 當將介面分配給區域時，將隱式阻止進出給定介面的所有流量，但進出同一區域中其他介面的流量以及到路由器上任何介面的流量除外。
- 預設情況下，隱式允許流量在屬於同一區域的介面之間流動。
- 為了允許流量進出區域成員介面，必須在該區域和任何其他區域之間配置允許或檢查流量的策略。
- 自區域是預設拒絕所有策略的唯一例外。在流量被顯式拒絕之前，允許所有到任何路由器介面的流量。
- 流量無法在區域成員介面和非區域成員的任何介面之間流動。通過、檢查和丟棄操作只能在兩個區域之間應用。
- 尚未指定給區域的介面用作經典路由器埠，並且仍然可以使用經典的有狀態檢測/CBAC配置。
- 如果要求機箱上的介面不屬於區域/防火牆策略的一部分。仍然必須將介面放入一個區域中，並在該區域和任何其它需要流量流區域之間配置全部通過策略（一種虛擬策略）。
- 根據前面的行為，如果流量要在路由器中的所有介面之間流動，則所有介面都必須是分割槽模型的一部分（每個介面必須是一個分割槽或另一個分割槽的成員）。
- 對於先前行為，預設拒絕方法的唯一例外是進出路由器的流量，預設情況下允許該流量。可以配置顯式策略來限制此類流量。

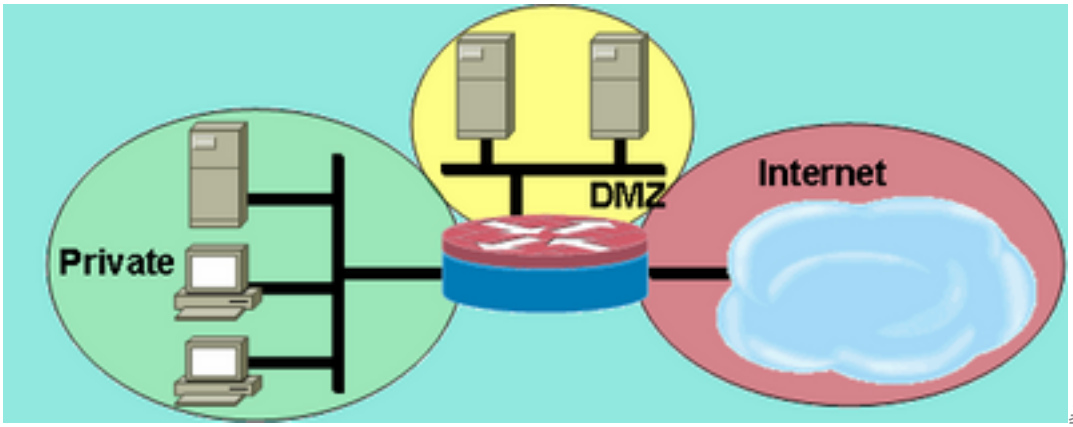
設計基於區域的策略網路安全

必須為網路內每個相對安全區域配置一個安全區域，以便分配給同一區域的所有介面都受到類似安全級別的保護。例如，假設接入路由器具有三個介面：

- 一個介面連線到公共Internet
- 一個連線到專用LAN的介面，不能從公共Internet訪問
- 一個介面連線到網際網路服務隔離區(DMZ)，公共網際網路必須可以訪問Web伺服器、域名系統(DNS)伺服器和電子郵件伺服器

此網路中的每個介面都分配給其自己的區域，但您可能希望允許從公共Internet到DMZ中特定主機的不同訪問，以及針對受保護LAN中主機的不同應用程式使用策略。（請參見圖1。）

圖1:基本安全區域拓撲



基本安全區域拓撲

在本例中，每個區域僅包含一個介面。如果將其他介面新增到專用區域，則連線到該區域中新介面的主機可以將流量傳送到同一區域中當前介面上的所有主機。此外，到其他區域中主機的主機流量同樣受當前策略的影響。

通常，示例網路有三個主要策略：

- 專用區域與Internet的連線
- 與DMZ主機的專用區域連線
- 與DMZ主機的網際網路區域連線

由於DMZ暴露於公共網際網路，因此DMZ主機可能會受到惡意個人的意外活動，這些惡意個人可能會成功損壞一台或多台DMZ主機。如果沒有為DMZ主機提供訪問策略以訪問專用區域主機或網際網路區域主機，則破壞DMZ主機的個人無法使用DMZ主機對專用或網際網路主機進行進一步攻擊。ZFW實施令人望而生畏的預設安全狀態。因此，除非專門為DMZ主機提供訪問其它網路的許可權，否則其它網路將免受來自DMZ主機的任何連線的威脅。同樣，不為Internet主機提供訪問專用區域主機的許可權，因此Internet主機可以安全地訪問專用區域主機。

將IPSec VPN與基於區域的策略防火牆配合使用

IPSec VPN的最新增強功能簡化了VPN連線的防火牆策略配置。IPSec虛擬通道介面(VTI)和GRE+IPSec允許通過將通道介面置於指定的安全區域來將VPN點對點連線和使用者端連線限制到特定安全區域。如果連線必須受特定策略的限制，可以在VPN DMZ中隔離連線。或者，如果VPN連線是隱式信任的，則可以將VPN連線置於與受信任的內部網路相同的安全區域。

如果應用了非VTI IPSec，則需要密切審查VPN連線防火牆策略以維護安全性。如果安全主機與VPN客戶端加密連線到路由器的區域不同，則區域策略必須特別允許遠端站點主機或VPN客戶端的IP地址訪問。如果訪問策略配置不當，必須保護的主機最終會暴露給不需要的潛在惡意主機。請參閱將VPN與基於區域的策略防火牆結合使用，瞭解進一步的概念和配置討論。

思科原則語言(CPL)組態

此過程可用於配置ZFW。步驟順序並不重要，但某些事件必須按順序完成。例如，在將類對映分配給策略對映之前，必須配置類對映。同樣，在配置策略之前，不能將策略對映分配給區域對。如果嘗試配置依賴未配置的另一部分配置的部分，路由器將發出錯誤消息。

1. 定義區域。
2. 定義區域對。
3. 定義類對映，此類對映描述跨區域對時必須應用策略的流量。
4. 定義策略對映以將操作應用於類對映流量。

5. 將策略對映應用於區域對。
6. 將介面分配給區域。

配置基於區域的策略防火牆類對映

類別對映定義防火牆為策略應用選擇的流量。第4層類對映根據此處列出的這些條件對流量進行排序。以下條件在類對映中通過match命令指定：

- Access-group — 標準ACL、擴展ACL或命名ACL可以根據源和目標IP地址以及源和目標埠過濾流量。
- Protocol — 第4層協定（TCP、UDP和ICMP）和應用服務（如HTTP、SMTP、DNS等）可以指定埠應用對映已知的任何已知或使用者定義的服務。
- Class-map — 提供其他匹配條件的從屬類對映可以巢狀在另一個類對映中。
- Not - not條件指定為類對映選擇與指定服務（協定）、訪問組或從屬類對映不匹配的任何流量。

合併「匹配」條件：「Match-Any」與「Match-All」

類對映可以應用match-any或match-all運算子來確定如何應用匹配條件。如果指定了match-any，則流量必須只滿足類對映中的一個匹配條件。如果指定match-all，則流量必須匹配所有類對映條件才能屬於該特定類。

如果流量滿足多個條件，則必須應用匹配條件，順序從更具體到不太具體。例如，請考慮以下類對映：

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

HTTP流量必須首先遇到匹配協定http，以確保通過HTTP檢查的服務特定功能處理流量。如果匹配行相反，則流量會遇到match protocol TCP語句，然後將其與match protocol http進行比較，然後將該流量簡單地分類為TCP流量，並根據防火牆TCP檢測元件的功能進行檢查。這對於某些服務(例如FTP、TFTP和多種多媒體和語音信令服務（例如H.323、SIP、Skinny、RTSP等）來說是個問題。這些服務需要額外的檢查能力，以識別這些服務的更複雜活動。

將ACL套用為匹配條件

類對映可以將ACL應用為策略應用的匹配條件之一。如果僅類對映匹配條件是ACL，且類對映與應用檢查操作的策略對映關聯，則路由器將對ACL允許的所有流量應用基本TCP或UDP檢查，但ZFW提供應用感知檢查的流量除外。其中包括（但不限於）FTP、SIP、Skinny(SCCP)、H.323、Sun RPC和TFTP。如果特定應用檢測可用，且ACL允許主要或控制通道，則無論該ACL是否允許流量，都允許與主要/控制相關聯的任何輔助或媒體通道。

如果類對映僅應用ACL 101作為匹配條件，則ACL 101顯示如下：

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

允許所有流量沿應用於給定區域對的服務策略方向傳輸，並且允許與此對應的返回流量沿相反方向傳輸。因此，ACL必須應用限制來將流量限制到特定的所需型別。請注意，PAM清單包括HTTP、NetBIOS、H.323和DNS等應用服務。但是，儘管PAM知道給定埠的特定應用程式使用，但防火牆僅應用足夠的應用程式特定功能來滿足應用程式流量的已知要求。因此，簡單應用流量（例如

telnet、SSH和其他單通道應用）會作為TCP進行檢查，並在show命令輸出中將這些應用的統計資訊組合在一起。如果需要特定於應用的網路活動可視性，則需要按應用名稱配置服務的檢查（配置匹配協定HTTP、匹配協定telnet等）。

將此配置輸出的show policy-map type inspect zone-pair命令輸出中的可用統計資訊與頁面下方所示的更明確的防火牆策略進行比較。此組態用於檢查來自Cisco IP電話以及使用各種流量（包括HTTP、FTP、NetBIOS、SSH和DNS）的若干工作站的流量：

```
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
```

雖然此配置易於定義並容納源自專用區域的所有流量（只要流量遵循標準、PAM識別的目的地埠），但它對服務活動的可視性有限，並且不能為特定型別的流量應用ZFW的頻寬和會話限制。此show policy-map type inspect zone-pair priv-pub命令輸出是先前簡單配置的結果，該配置在區域對之間僅使用permit IP [subnet] any ACL。您可以看到，大部分工作站流量都計入基本TCP或UDP統計資訊中：

```
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
```

相比之下，新增特定於應用程式的類的類似配置可以提供更精細的應用程式統計資訊和控制，並且仍然可以容納與定義最後機會類對映時第一個示例中顯示的服務範圍相同的服務，該對映僅匹配ACL作為策略對映中的最後機會：

```
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
```

更具體一些的配置為show policy-map type inspect zone-pair priv-pub命令提供這種細粒度輸出：

```
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
```

如前所述，如果使用更精細的類對映和策略對映配置，還有另一個額外優勢：可以對會話和速率值應用特定於類的限制；通過應用引數對映來調整各類檢測行為，從而對檢測引數進行具體調整。

配置基於區域的策略防火牆策略對映

策略對映將防火牆策略操作應用於一個或多個類對映，以定義應用於安全區域對的服務策略。建立inspect-type policy-map時，在類的末尾應用名為class class class-default的預設類。class class-default預設策略操作為drop，但可以更改為pass。日誌選項可以與刪除操作一起新增。無法在class class-default上應用檢查。

基於區域的策略防火牆操作

ZFW為從一個區域到另一個區域的流量提供三種操作：

- Drop — 這是所有流量的預設操作，由終止每個檢查型別策略對映的class class-default應用。也可以將策略對映中的其他類對映配置為丟棄不需要的流量。ZFW會靜默捨棄由捨棄操作處理的流量（也就是不會將捨棄通知傳送到相關終端主機），這與ACL行為相反，當ZFW向傳送拒絕流量的主機傳送ICMP「主機無法連線」訊息時。目前，沒有更改靜默丟棄行為的選項。日誌選項可以新增drop以通知系統日誌流量被防火牆丟棄。

- 通過 — 此操作允許路由器將流量從一個區域轉發到另一個區域。傳遞操作不跟蹤流量內的連線或會話狀態。Pass僅允許單向流量。必須應用並行策略以允許返回流量反向通過。pass操作對於協定（例如IPSec ESP、IPSec AH、ISAKMP）和其他本身具有可預測行為的安全協定非常有用。但是，大多數應用流量在ZFW中通過檢查操作得到更好的處理。
- Inspect — 檢查操作提供基於狀態的流量控制。例如，如果檢查從先前範例網路中的私人區域到Internet區域的流量，路由器會維護TCP和使用者資料包通訊協定(UDP)流量的連線或作業階段資訊。因此，路由器允許從Internet區域主機傳送返回流量來響應專用區域連線請求。此外，檢查可以為可能承載易受攻擊或敏感應用流量的某些服務協定提供應用檢查和控制。可以使用引數對映應用審計追蹤，以記錄連線/會話的開始、停止、持續時間、傳輸的資料量以及源地址和目標地址。

操作與策略對映中的類對映關聯：

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

引數對映提供用於修改給定類對映檢查策略的連線引數的選項。

配置區域策略防火牆引數對映

引數對映指定ZFW的檢查行為，例如DoS保護、TCP連線/UDP會話計時器和審計跟蹤日誌記錄設定等引數。引數對映還與第7層類和策略對映一起應用，以定義應用程式特定的行為，如HTTP對象、POP3和IMAP身份驗證要求以及其他應用程式特定的資訊。

ZFW的檢查引數對映配置為型別inspect，類似於其他ZFW類和策略對象：

```
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
```

特定型別的引數對映指定第7層應用檢查策略應用的引數。Regex型別引數對映定義正規表示式，用於使用正規表示式過濾流量的HTTP應用檢測：

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

Protocol-info-type parameter-maps定義用於IM應用程式檢查的伺服器名稱：

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

HTTP和IM應用檢測的完整配置詳細資訊請參見本文檔的各個應用檢測部分。

對基於區域的策略防火牆策略應用日誌記錄

ZFW為預設丟棄或檢查的流量或配置的防火牆策略操作提供日誌記錄選項。稽核跟蹤日誌記錄可用於ZFW檢查的流量。在引數對映中定義稽核跟蹤並在策略對映中應用具有檢查操作的引數對映時，將應用稽核跟蹤：

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

丟棄日誌記錄可用於ZFW丟棄的流量。在策略對映中新增帶有丟棄操作的日誌時，會配置丟棄日誌記錄：

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

編輯區域策略防火牆類對映和策略對映

ZFW目前沒有可以修改各種ZFW結構（如策略對映、類對映和引數對映）的編輯器。若要將類對映或操作應用程式中的match語句重新排列到策略對映中包含的各種類對映，需要完成以下步驟：

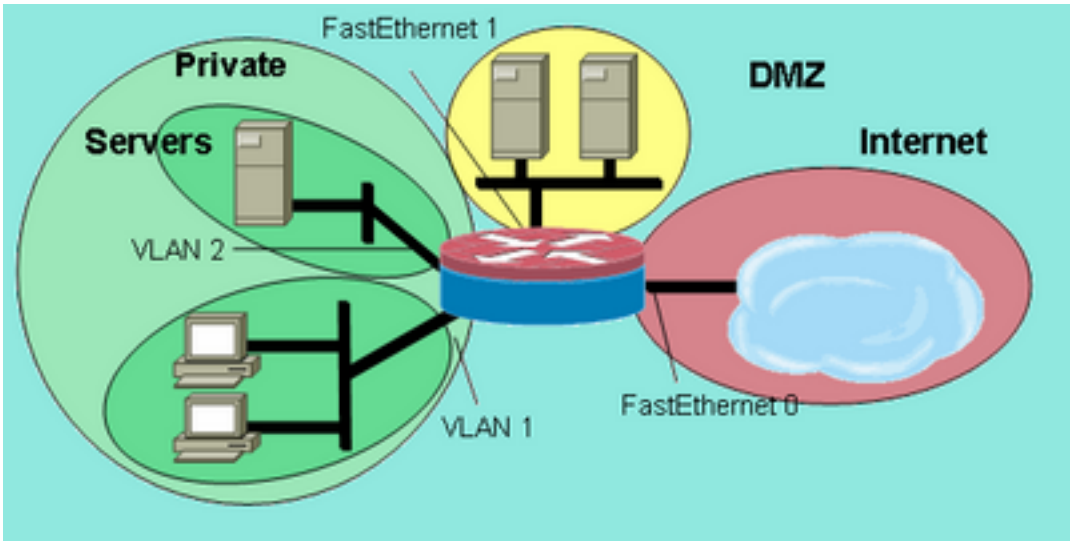
1. 將當前結構複製到文本編輯器（如Microsoft Windows記事本）或編輯器（如Linux/Unix平台上的vi）。
2. 從路由器配置中刪除當前結構。
3. 在文本編輯器中編輯結構。
4. 將結構複製迴路由器CLI。

組態範例

此配置示例使用Cisco 1811整合多業務路由器。附錄A提供了兩個專用乙太網LAN網段之間具有IP連線、VLAN配置和透明橋接的基本配置資訊。路由器分為五個區域：

- 公共Internet連線到FastEthernet 0（Internet區域）
- 兩台網際網路伺服器連線到FastEthernet 1（DMZ區域）
- 乙太網交換機配置了兩個VLAN:工作站連線到VLAN1（客戶端區域）。伺服器連線到VLAN2（伺服器區域）。客戶端和伺服器區域位於同一個子網中。在區域之間應用透明防火牆，因此這兩個介面上的區域間策略只能影響客戶端和伺服器區域之間的流量。
- VLAN1和VLAN2介面通過網橋虛擬介面(BVI1)與其他網路通訊。 此介面分配給專用區域。（請參見圖2。）

圖2:區域拓撲詳細資訊

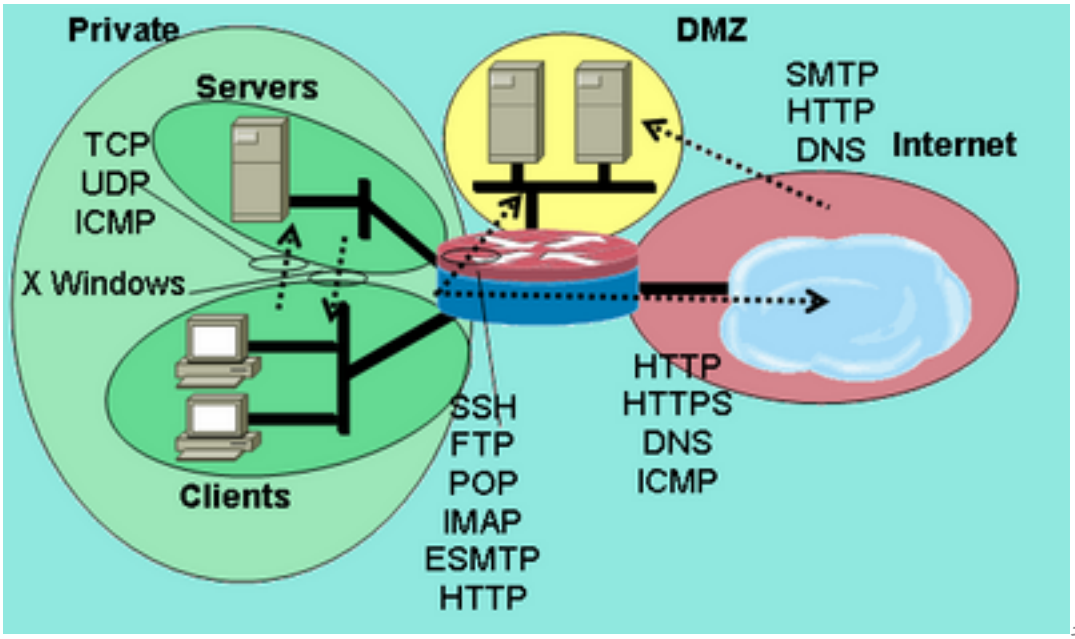


區域拓撲詳細資訊

應用以下策略，並應用前面定義的網路區域：

- Internet區域中的主機可以到達DMZ中一台伺服器上的DNS、SMTP和SSH服務。另一台伺服器提供SMTP、HTTP和HTTPS服務。防火牆策略限制對每台主機上可用特定服務的訪問。
- DMZ主機無法連線到任何其他區域中的主機。
- 客戶端區域中的主機可以連線到伺服器區域中的所有TCP、UDP和ICMP服務上的主機。
- 伺服器區域中的主機無法連線到客戶端區域中的主機，但基於UNIX的應用程式伺服器可以開啟到客戶端區域埠6900到6910上案頭PC上的X Windows伺服器的X Windows客戶端會話。
- 專用區域中的所有主機（客戶端和伺服器的組合）都可以訪問DMZ中的SSH、FTP、POP、IMAP、ESMTP和HTTP服務主機，以及HTTP、HTTPS、DNS服務和ICMP上的Internet區域中的主機。此外，對從專用區域到Internet區域的HTTP連線應用檢查，以確保支援的IM和P2P應用不在埠80上傳輸。（參見圖3。）

圖3:要在配置示例中應用的區域對服務許可權



要在配置示例中應用的區域對服務許可權

這些防火牆策略按複雜程度進行配置：

1. 客戶端 — 伺服器TCP/UDP/ICMP檢測
2. Private-DMZ SSH/FTP/POP/IMAP/ESMTP/HTTP檢測

3. Internet — 受主機地址限制的DMZ SMTP/HTTP/DNS檢查
4. 伺服器 — 客戶端X Windows檢查及埠應用程式對映(PAM)指定的服務
5. 含HTTP應用程式檢查的專用網際網路HTTP/HTTPS/DNS/ICMP

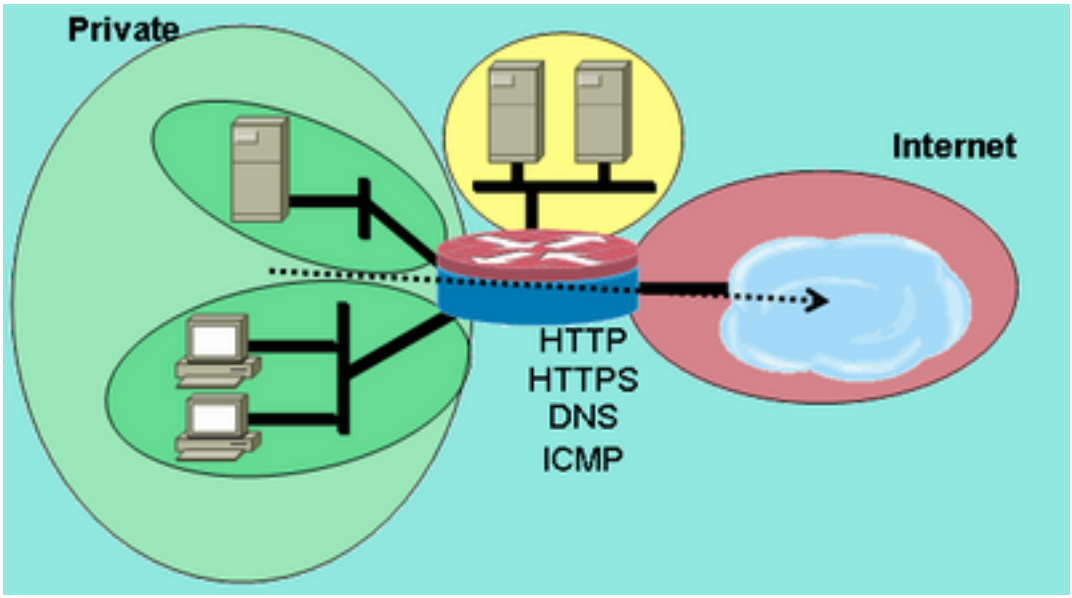
由於您在不同時間將部分配置應用到不同的網段，因此請務必記住，當網段置於區域中時，該網段會失去與其它網段的連線。例如，配置專用區域後，專用區域中的主機將失去與DMZ和網際網路區域的連線，直到定義了各自的策略。

狀態檢測路由防火牆

配置專用Internet策略

圖4顯示了專用Internet策略的配置。

圖4:從專用區域到Internet區域的服務檢查



從專用區域到Internet區域的服務檢查

專用Internet策略對從專用區域到Internet區域的ICMP的HTTP、HTTPS、DNS和第4層檢測應用第4層檢測。這樣允許從專用區域到Internet區域的連線，並允許返回流量。第7層檢查具有更緊密的應用程式控制、更好的安全性和對需要修復的應用程式的支援的優點。但是，如前所述，第7層檢測需要更好地瞭解網路活動，因為區域之間不允許配置未進行檢測的第7層協定。

1. 根據前面所述的策略，定義描述要在區域之間允許的流量的類對映：
```
configure terminal
 class-map type inspect match-any internet-traffic-class
  match protocol http
  match protocol https
  match protocol dns
  match protocol icmp
```
2. 配置策略對映以檢查剛剛定義的類對映上的流量：
```
configure terminal
 policy-map type inspect private-internet-policy
  class type inspect internet-traffic-class
   inspect
```
3. 配置專用區域和Internet區域，並將路由器介面分配給其各自的區域：
```
configure terminal
 zone security private
 zone security internet
```

```
int bvi1
 zone-member security private
int fastethernet 0
 zone-member security internet
```

配置區域對並應用適當的策略對映。

附註：您目前只需配置專用Internet區域對，即可檢查源自Internet專用區域的連線，該專用區域會傳輸到Internet區域，如下所示：

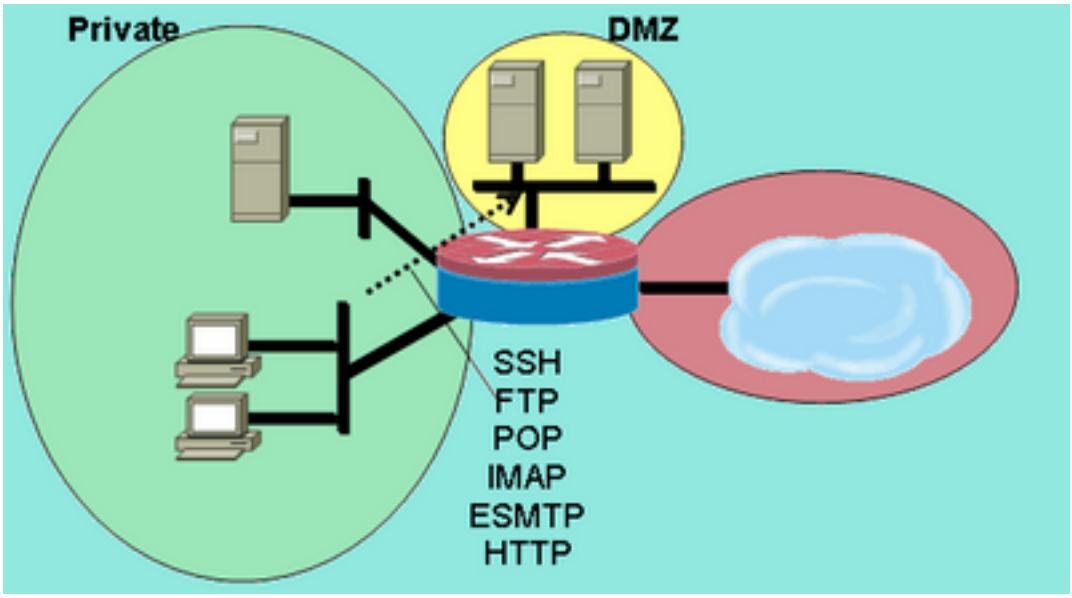
```
configure terminal
 zone-pair security private-internet source private destination internet
  service-policy type inspect private-internet-policy
```

這將完成專用Internet區域對上的第7層檢測策略的配置，以允許從客戶端區域到伺服器區域的HTTP、HTTPS、DNS和ICMP連線，並對該HTTP流量應用應用檢測，以確保不允許不需要的流量通過TCP 80（HTTP的服務埠）。

配置專用DMZ策略

圖5顯示了專用DMZ策略的配置。

圖5:從專用區域到DMZ區域的服務檢查



從專用區域到DMZ區域的服務檢查

專用DMZ策略增加了複雜性，因為它需要更好地瞭解區域之間的網路流量。此策略將第7層檢測從專用區域應用到DMZ。這樣允許從專用區域到DMZ的連線，並允許返回流量。第7層檢查具有更緊密的應用程式控制、更好的安全性和對需要修復的應用程式的支援的優點。但是，如前所述，第7層檢測需要更好地瞭解網路活動，因為區域之間不允許配置未進行檢測的第7層協定。

1. 根據前面所述的策略，定義描述要在區域之間允許的流量的類對映：

```
configure terminal
 class-map type inspect match-any L7-inspect-class
  match protocol ssh
  match protocol ftp
  match protocol pop
  match protocol imap
  match protocol esmtp
```

```
  match protocol http
```

2. 配置策略對映以檢查您剛才定義的類對映上的流量：

```
configure terminal
 policy-map type inspect private-dmz-policy
  class type inspect L7-inspect-class
   inspect
```

3. 配置專用區域和DMZ區域，並將路由器介面分配給各自的區域：

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

4. 配置區域對並應用適當的策略對映。

附註：您目前只需配置專用DMZ區域對，即可檢查源自DMZ專用區域的連線，如下所示：

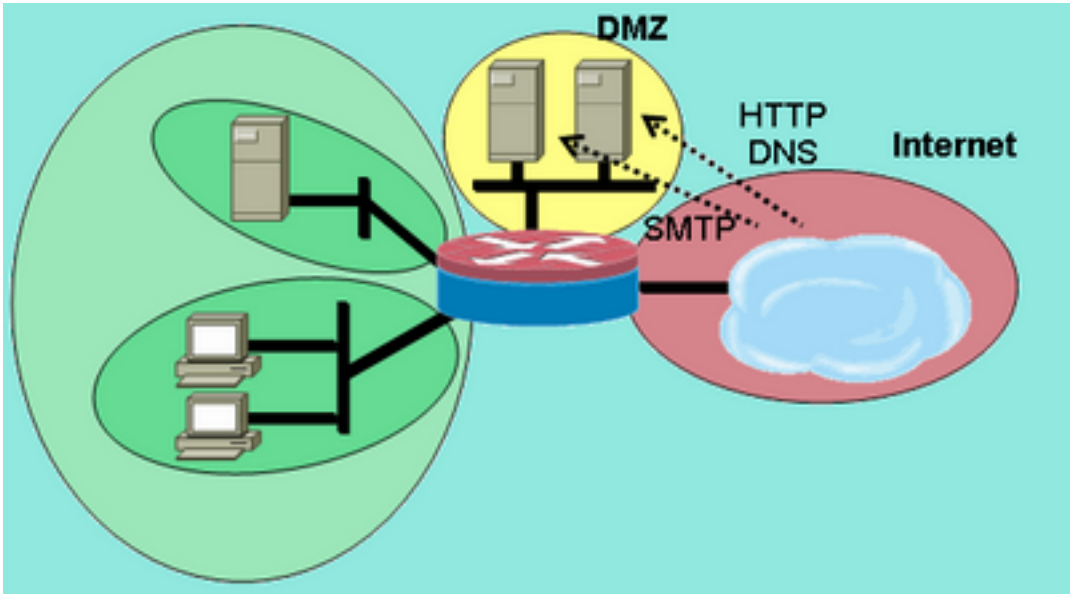
```
configure terminal
 zone-pair security private-dmz source private destination dmz
  service-policy type inspect private-dmz-policy
```

這將完成專用DMZ上的第7層檢測策略的配置，以允許從客戶端區域到伺服器區域的所有TCP、UDP和ICMP連線。該策略不會對從屬通道應用修復，但提供了一個簡單策略示例，可適應大多數應用程式連線。

配置網際網路DMZ策略

圖6顯示了網際網路DMZ策略的配置。

圖6:從Internet區域到DMZ區域的服務檢查



從Internet區域到DMZ區域的服務檢查

此策略將第7層檢測從網際網路區域應用到DMZ。這允許從Internet區域到DMZ的連線，並允許從DMZ主機到發起連線的網際網路主機的返回流量。Internet DMZ策略將第7層檢測與ACL定義的地址組相結合，以限制對特定主機、主機組或子網上的特定服務的訪問。要實現此目的，需要巢狀一個類對映，該類對映在另一個類對映中指定服務，該類對映引用ACL來指定IP地址。

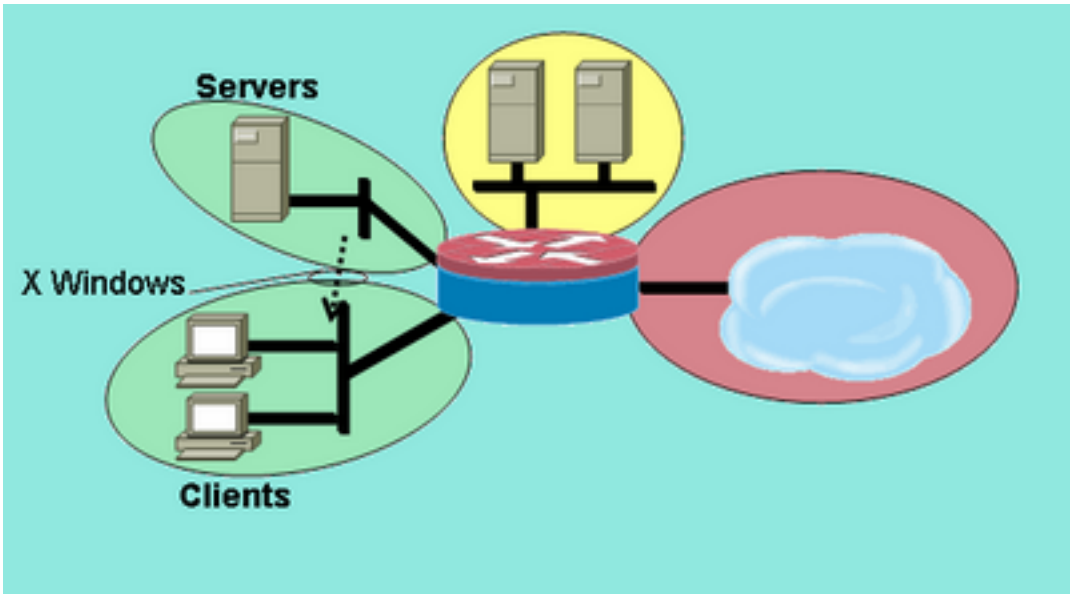
1. 根據前面所述的策略，定義類對映和ACL，以描述要在區域之間允許的流量。必須使用服務的多個類對映，因為對兩個不同伺服器的訪問應用不同的訪問策略。允許Internet主機通過DNS和HTTP連線到達172.16.2.2，允許SMTP連線到達172.16.2.3。請注意類別對映的差異。指定服務的類對映使用match-any關鍵字允許列出的任何服務。將ACL與服務類對映關聯的類對映使用match-all關鍵字來要求必須滿足類對映的兩個條件才能允許流量：
```
configure terminal
 access-list 110 permit ip any host 172.16.2.2
 access-list 111 permit ip any host 172.16.2.3
 class-map type inspect match-any dns-http-class
  match protocol dns
  match protocol http
 class-map type inspect match-any smtp-class
  match protocol smtp
 class-map type inspect match-all dns-http-acl-class
  match access-group 110
  match class-map dns-http-class
 class-map type inspect match-all smtp-acl-class
  match access-group 111
  match class-map smtp-class
```
2. 配置策略對映以檢查您剛才定義的類對映上的流量：
```
configure terminal
 policy-map type inspect internet-dmz-policy
  class type inspect dns-http-acl-class
   inspect
  class type inspect smtp-acl-class
   inspect
```
3. 配置Internet和DMZ區域並將路由器介面分配給其各自的區域。如果在上一節中設定DMZ配置，請跳過該配置：
```
configure terminal
zone security internet
zone security dmz
int fastethernet 0
 zone-member security internet
int fastethernet 1
 zone-member security dmz
```
4. 配置區域對並應用適當的策略對映。**附註**：您目前只需配置Internet DMZ區域對，即可檢查源自Internet區域且流向DMZ區域的連線，如下所示：
```
configure terminal
 zone-pair security internet-dmz source internet destination dmz
  service-policy type inspect internet-dmz-policy
```
這將完成網際網路DMZ區域對上特定於地址的第7層檢測策略的配置。

狀態檢測透明防火牆

配置伺服器 — 客戶端策略

下圖說明了伺服器客戶端策略的配置。

圖7:從伺服器區域到客戶端區域的服務檢查



從伺服器區域到客戶端區域的服務檢查

servers-clients策略對使用者定義的服務應用檢測。第7層檢測從伺服器區域應用到客戶端區域。這允許X Windows連線到從伺服器區域到客戶端區域的特定埠範圍，並允許返回流量。X Windows在PAM中不是本機支援的協定，因此必須在PAM中定義使用者配置的服務，以便ZFW可以識別並檢查適當的流量。

在IEEE網橋組中配置兩個或多個路由器介面以提供整合路由和橋接(IRB)，以便在網橋組中的介面之間提供橋接，並通過網橋虛擬介面(BVI)路由到其他子網。 透明防火牆策略對通過「網橋」的流量應用防火牆檢查，但不對通過BVI離開網橋組的流量應用防火牆檢查。檢查策略僅適用於通過網橋組的流量。因此，在此場景中，檢測僅應用於在客戶端和伺服器區域之間移動的流量，這些流量巢狀在專用區域內。僅當流量通過BVI離開網橋組時，在專用區域、公共區域和DMZ區域之間應用的策略才會發揮作用。當流量通過BVI從客戶端或伺服器區域離開時，不會呼叫透明防火牆策略。

1. 為X Windows配置使用者定義的PAM。X Windows客戶端（其中承載應用程式）開啟連線，從埠6900開始的範圍內向客戶端（使用者工作的地方）顯示資訊。每個附加連線都使用連續埠，因此，如果客戶端在一台主機上顯示10個不同的會話，則伺服器使用埠6900-6909。因此，如果您檢查從6900到6909的埠範圍，開啟到6909以外埠的連線將失敗：
```
configure terminal
 ip port-map user-Xwindows port tcp from 6900 to 6910
```
2. 檢視PAM文檔以解決其他PAM問題，或檢查精細協定檢查文檔，瞭解有關PAM和Cisco IOS防火牆狀態檢測之間互操作性的詳細資訊。
3. 根據前面所述的策略，定義描述要在區域之間允許的流量的類對映：
```
configure terminal
 class-map type inspect match-any Xwindows-class
  match protocol user-Xwindows
```
4. 配置策略對映以檢查您剛才定義的類對映上的流量：
```
configure terminal
 policy-map type inspect servers-clients-policy
  class type inspect Xwindows-class
   inspect
```
5. 配置客戶端和伺服器區域，並將路由器介面分配給其各自的區域。如果在Clients-Servers Policy Configuration部分配置了這些區域和分配的介面，則可以跳至區域對定義。為完整性提供了橋接IRB配置：
```
configure terminal
bridge irb
bridge 1 protocol ieee
bridge 1 route ip
zone security clients
```

```
zone security servers
 int vlan 1
 bridge-group 1
 zone-member security clients
int vlan 2
 bridge-group 1
 zone-member security servers
```

6. 配置區域對並應用適當的策略對映。**附註**：您目前只需配置servers-clients區域對，即可檢查源自servers區域中的到達客戶端區域的連線，如下所示：

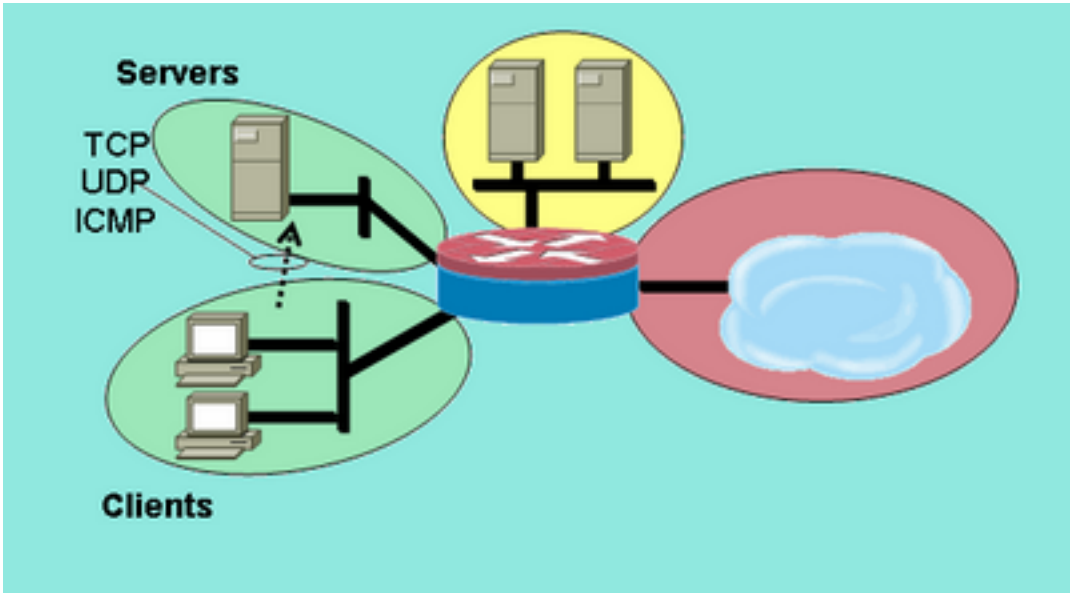
```
configure terminal
 zone-pair security servers-clients source servers destination clients
  service-policy type inspect servers-clients-policy
```

這將完成servers-clients區域對中使用者定義的檢查策略的配置，以允許從伺服器區域到客戶端區域的X Windows連線。

配置客戶端 — 伺服器策略

圖8說明了客戶端 — 伺服器策略的配置。

圖8:從客戶端區域到伺服器區域的服務檢查



從客戶端區域到伺服器區域的服務檢查

客戶端 — 伺服器策略比其他策略更簡單。第4層檢測從客戶端區域應用到伺服器區域。這允許從客戶端區域到伺服器區域的連線，並允許返回流量。第4層檢測具有防火牆配置簡便的優點，因為只需要一些規則即可允許大多數應用流量。但是，第4層檢查也有兩個主要缺點：

- FTP或媒體服務等應用經常協商從伺服器到客戶端的附加從屬通道。此功能通常包含在監控控制通道對話方塊並允許從屬通道的服務修復中。此功能在第4層檢測中不可用。
- 第4層檢測允許幾乎所有應用層流量。如果必須控制網路使用，以便僅允許少數應用通過防火牆，則必須在出站流量上配置ACL，以限制允許通過防火牆的服務。

兩個路由器介面都配置在IEEE網橋組中，因此此防火牆策略應用透明防火牆檢測。此策略應用於IEEE IP網橋組中的兩個介面。檢查策略僅適用於通過網橋組的流量。這解釋了客戶端和伺服器區域巢狀在專用區域內的原因。

1. 根據前面所述的策略，定義描述要在區域之間允許的流量的類對映：

```
configure terminal
 class-map type inspect match-any L4-inspect-class
```

```
 match protocol tcp
 match protocol udp
 match protocol icmp
```

2. 配置策略對映以檢查您剛才定義的類對映上的流量：

```
configure terminal
 policy-map type inspect clients-servers-policy
 class type inspect L4-inspect-class
  inspect
```

3. 配置客戶端和伺服器區域並將路由器介面分配給其各自的區域：

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

4. 配置區域對並應用適當的策略對映。**附註**：您目前只需配置clients-servers區域對，即可檢查源自clients區域中到達伺服器區域的連線，如下所示：

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

這樣就完成了客戶端 — 伺服器區域對的第4層檢測策略的配置，以允許從客戶端區域到伺服器區域的所有TCP、UDP和ICMP連線。該策略不會對從屬通道應用修正，但提供了一個簡單策略示例，可適應大多數應用程式連線。

基於區域的策略防火牆的速率策略

資料網路通常能夠限制特定網路流量型別的傳輸速率，並限制較低優先順序的流量對更多業務關鍵型流量的影響，因而受益。Cisco IOS軟體通過流量管制（可限制流量標稱速率和突發）提供此功能。Cisco IOS軟體自Cisco IOS版本12.1(5)T起支援流量管制。

當您新增功能來管制與特定類別對映的定義相匹配的流量時，當您從一個安全區域穿越防火牆到另一個安全區域時，Cisco IOS軟體版本12.4(9)T為ZFW增加了速率限制功能。這樣便可以通過一個配置點來描述特定流量、應用防火牆策略並管制流量頻寬消耗。ZFW與基於介面的不同之處在於，它只提供為策略一致性而傳輸的操作，以及為策略違規而丟棄的操作。ZFW無法標籤DSCP的流量。

ZFW只能以位元組/秒、資料包/秒為單位指定頻寬使用，並且不提供頻寬百分比。ZFW可以應用基於介面或不應用基於介面的。因此，如果需要其他功能，這些功能可以通過基於介面應用。如果基於介面與防火牆結合使用，請確保策略不衝突。

配置ZFW策略

ZFW策略將策略對映類對映中的流量限製為使用者定義的速率值，範圍在8,000到2,000,000,000位/秒之間，可配置的突發值在1,000到512,000,000位元組之間。

ZFW策略由策略對映中的另一行配置配置，該配置在策略操作之後應用：

```
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>]
```

作業階段控制

ZFW策略還引入了會話控制，以限制應用與類對映匹配的策略對映中流量的會話計數。這增加了當前為每個類對映應用DoS保護策略的功能。實際上，這允許精細地控制應用與任何跨越區域對的給定類對映匹配的會話數量。如果在多個策略對映或區域對上使用相同的類對映，則可以在各種類對映應用上應用不同的會話限制。

當配置包含所需會話卷的引數對映時，應用會話控制，然後將引數對映附加到策略對映下應用於類對映的檢查操作：

```
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
```

引數對映只能應用於檢查操作，不能用於傳遞或丟棄操作。

使用以下命令可以看到ZFW會話控制和策略活動：

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

應用檢測

應用檢測為ZFW引入了附加功能。應用檢查策略應用在OSI模型的第7層，在該層中，使用者應用傳送和接收消息，使應用能夠提供有用的功能。某些應用程式可以提供不需要的或易受攻擊的功能，因此必須過濾與這些功能相關的消息，以限制應用程式服務上的活動。

Cisco IOS軟體ZFW提供以下應用服務的應用檢測和控制：

- HTTP
- SMTP
- POP3
- IMAP
- Sun RPC
- P2P應用流量
- 即時消息應用

應用檢測和控制(AIC)的功能因服務而異。HTTP檢查提供對多種型別的應用程式活動的精細過濾，並提供限制傳輸大小、Web地址長度和瀏覽器活動的功能，以強制遵守應用程式行為標準並限制通過服務傳輸的內容型別。用於SMTP的AIC可以限制內容長度並實施協定合規性。POP3和IMAP檢查可幫助確保使用者使用安全身份驗證機制來防止使用者憑據受損。

應用檢測配置為一組額外的應用特定類對映和策略對映，當您在檢測策略對映中定義應用服務策略時，這些對映將應用於當前檢測類對映和策略對映。

HTTP應用檢測

可以對HTTP流量應用應用檢測，以控制其他應用（例如IM、P2P檔案共用和隧道應用）不需要的使用HTTP服務埠，這些應用可以通過TCP 80重定向其他防火牆應用。

配置應用檢測類對映以描述違反允許HTTP流量的流量：

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

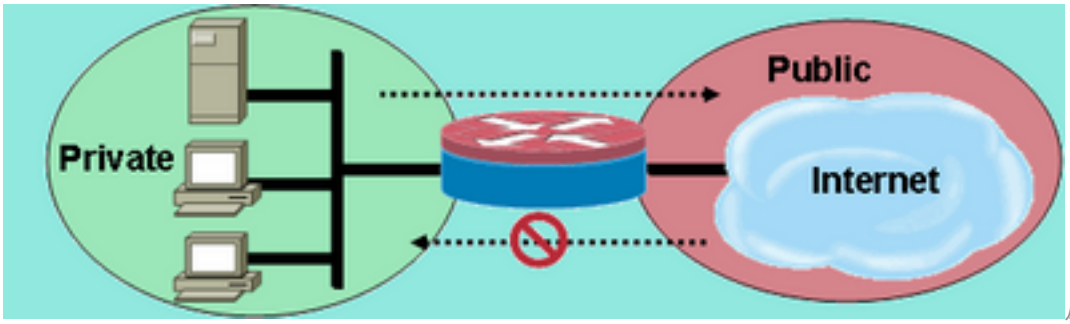
HTTP應用檢測改進

Cisco IOS軟體版本12.4(9)T對ZFW HTTP檢查功能進行了改進。Cisco IOS防火牆在Cisco IOS軟體版本12.3(14)T中引入了HTTP應用程式檢查。當您新增以下內容時，Cisco IOS軟體版本12.4(9)T擴充了目前的功能：

- 能夠根據報頭名稱和報頭值允許、拒絕和監控請求和響應。這對於阻止帶有易受攻擊的報頭欄位的請求和響應非常有用。
- 能夠限制HTTP請求和響應報頭中不同元素的大小，如最大URL長度、最大報頭長度、最大報頭數、最大報頭行長度等。這對於防止緩衝區溢位非常有用。
- 能夠阻止攜帶同一型別多個標頭的請求和響應；例如，包含兩個內容長度標頭的請求。
- 能夠阻止具有非ASCII標頭的請求和響應。這對於防止使用二進位制和其他非ASCII字元將蠕蟲和其他惡意內容傳送到Web伺服器的各種攻擊非常有用。
- 能夠將HTTP方法分組到使用者指定的類別，並靈活地阻止/允許/監視每個組。HTTP RFC允許一組受限制的HTTP方法。有些標準方法被認為是不安全的，因為它們可用於利用Web伺服器上的漏洞。許多非標準方法都有不良的安全記錄。
- 根據使用者配置的正規表示式阻止特定URI的方法。此功能使使用者能夠阻止自定義URI和查詢。
- 能夠使用使用者可自定義的字串偽裝報頭型別（特別是伺服器報頭型別）。在攻擊者分析Web伺服器響應並獲取儘可能多的資訊，然後發起攻擊以利用特定Web伺服器中的弱點的情況下，此功能非常有用。
- 如果一個或多個HTTP引數值與使用者作為正規表示式輸入的值匹配，則能夠阻止或發出HTTP連線警報。一些可能的HTTP值上下文包括報頭、正文、使用者名稱、密碼、使用者代理、請求行、狀態行和解碼CGI變數。

HTTP應用檢測改進的配置示例假定網路簡單，如圖9所示。

圖9:應用檢測假定網路簡單



應用檢測假定網路簡單

防火牆將流量分為兩類：

- HTTP流量
- 所有其他單通道TCP、UDP和ICMP流量

HTTP是分開的，以允許對Web流量進行特定檢測。這樣，您便可以在本文檔的第一部分中配置策略，並在第二部分中配置HTTP應用檢測。您可以在本文檔的第三部分中為P2P和IM流量配置特定類對映和策略對映。允許從專用區域連線到公共區域。未提供從公共區域到專用區域的連線。

請參閱附錄C獲取實施初始策略的完整配置。

配置HTTP應用檢測增強功能

HTTP應用檢測（以及其他應用檢測策略）需要比基本第4層配置更複雜的配置。您必須配置第7層流量分類和策略，以識別要控制的特定流量，並將所需操作應用於所需和不需要的流量。

HTTP應用檢測（類似於其他型別的應用檢測）只能應用於HTTP流量。因此，您必須為特定HTTP流量定義第7層類對映和策略對映，然後為特定HTTP定義第4層類對映，並將第7層策略應用於第4層策略對映中的HTTP檢查，如下所示：

```
!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
```

所有這些HTTP應用檢測流量特性都在第7層類對映中定義：

- 報頭檢查命令提供允許/拒絕/監視其報頭與配置的正規表示式匹配的請求或響應的功能。允許或重置操作可應用於符合類對映條件的請求或響應。新增日誌操作會導致系統日誌消息：

APPFW-6-HTTP_HDR_REGEX_MATCHED

命令用法：

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

用例示例

- 配置http appfw策略以阻止其標頭包含非ASCII字元的請求或響應。

```
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
```

報頭長度檢查 — 此命令檢查請求或響應報頭的長度，如果長度超過配置的閾值，將應用操作。允許或重置操作。新增日誌操作會導致系統日誌消息：

```
APPFW-4- HTTP_HEADER_LENGTH
```

命令用法：

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

用例示例

配置http appfw策略以阻止報頭長度大於4096位元組的請求和響應。

```
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
```

報頭計數檢查 — 此命令驗證請求/響應中的報頭行（欄位）數量，並在計數超過配置的閾值時應用操作。允許或重置操作。新增日誌操作會導致系統日誌消息：

```
APPFW-6- HTTP_HEADER_COUNT
```

命令用法：

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

用例示例

配置http appfw策略以阻止具有超過16個報頭欄位的請求。

```
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
```

報頭欄位檢測 — 此命令提供允許/拒絕/監控包含特定HTTP報頭欄位和值的請求/響應的功能。允許或重置操作可應用於符合類對映條件的請求或響應。新增日誌操作會導致系統日誌消息：

```
APPFW-6- HTTP_HDR_FIELD_REGEX_MATCHED
```

命令用法：

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

用例示例

配置HTTP應用程式檢查策略以阻止間諜軟體/廣告軟體：

```
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
```

報頭欄位長度檢查 — 此命令可限制報頭欄位行的長度。允許或重置操作可應用於符合類對映條件的請求或響應。新增日誌操作會導致系統日誌消息：

```
APPFW-6- HTTP_HDR_FIELD_LENGTH
```

命令用法：

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

用例示例

配置http appfw策略以阻止其cookie和使用者代理欄位長度分別超過256和128的請求。

```
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
```

檢查報頭欄位重複 — 此命令檢查請求或響應是否具有重複的報頭欄位。允許或重置操作可應用於符合類對映條件的請求或響應。啟用後，日誌操作將生成系統日誌消息：

APPFW-6- HTTP_REPEATED_HDR_FIELDS

命令用法：

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

用例示例

配置http appfw策略以阻止具有多個內容長度報頭行的請求或響應。這是用於防止會話走私的最有用的功能之一。

```
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
```

- 方法檢查 — HTTP RFC允許一組受限制的HTTP方法。但是，即使有些標準方法也被認為是不安全的，因為有些方法可以用來利用Web伺服器上的漏洞。許多非標準方法經常用於惡意活動。這就需要將這些方法分為不同的類別，並讓使用者為每個類別選擇操作。此命令為使用者提供了一種靈活的方法，可將方法分為各種類別，例如安全方法、不安全方法、webdav方法、RFC方法和擴展方法。允許或重置操作可應用於符合類對映條件的請求或響應。新增日誌操作會導致系統日誌消息：

APPFW-6-HTTP_METHOD

命令用法：

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

用例示例

配置http appfw策略，將HTTP方法分為三類：安全、不安全和webdav。這些內容顯示在下表中。配置以下操作：

- 允許所有安全方法而不包含日誌
- 所有不安全的方法都允許在日誌中使用
- 所有webdav方法都被log阻止。

安全	不安全	WebDAV
GET、HEAD、OPTION	POST、PUT、CONNECT、TRACE	BCOPY、BDELETE、BMOVE

```
http policy:

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

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

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

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

URI檢查 — 此命令提供允許/拒絕/監視其URI與配置的常規檢查相匹配的請求的能力。這允許使用者阻止自定義URL和查詢。允許或重置操作可應用於符合類對映條件的請求或響應。新增日誌操作會導致系統日誌消息：

```
APPFW-6- HTTP_URI_REGEX_MATCHED
```

命令用法：

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

用例示例

配置http appfw策略以阻止其URI匹配以下任何正規表示式的請求：

- .*cmd.exe
- .*性
- .*賭博

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

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

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

- URI長度檢查 — 此命令驗證請求中傳送的URI的長度，並在長度超過配置的閾值時應用配置的操作。允許或重置操作可應用於符合類對映條件的請求或響應。新增日誌操作會導致系統日誌消息：

  ```
  APPFW-6- HTTP_URI_LENGTH
  ```

  命令用法：

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

  用例示例

配置http appfw策略，以便在請求的URI長度超過3076位元組時發出警報。

```
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
```

引數檢查 — 此命令提供允許、拒絕或監視其引數（引數）與配置的常規檢查相匹配的請求的能力。允許或重置操作可應用於符合類對映條件的請求或響應。新增日誌操作會導致系統日誌消息：

```
APPFW-6- HTTP_ARG_REGEX_MATCHED
```

命令用法：

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

配置http appfw策略以阻止其引數與以下任何正規表示式匹配的請求：

- .*編碼
- .*攻擊

```
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
```

- 引數長度檢查 — 此命令驗證在請求中傳送的引數的長度，並在長度超過配置的閾值時應用配置的操作。允許或重置操作可應用於符合類對映條件的請求或響應。新增日誌操作會導致系統日誌消息：

  ```
  APPFW-6- HTTP_ARG_LENGTH
  ```

  命令用法：

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

  用例示例

配置http appfw策略以在請求的引數長度超過512位元組時發出警報。

```
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
```

- 正文檢查 — 此CLI允許使用者指定正規表示式的清單，以便與請求或響應的正文進行匹配。允許或重置操作可應用於符合類對映條件的請求或響應。新增日誌操作會導致系統日誌消息：

  ```
  APPFW-6- HTTP_BODY_REGEX_MATCHED
  ```

  命令用法：

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

  用例示例

配置http appfw以阻止其主體包含模式。`*[Aa][Tt][Tt][Aa][Cc][Kk]`

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

class-map type inspect http body_match_cm
```

```
   match response body regex body_regex

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

正文（內容）長度檢查 — 此命令驗證通過請求或響應傳送的消息的大小。允許或重置操作可應用於符合類對映條件的請求或響應。新增日誌操作會導致系統日誌消息：

```
APPFW-4- HTTP_CONTENT_LENGTH
```

命令用法：

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

用例示例

配置http appfw策略以阻止請求或響應中攜帶超過10K位元組消息的http會話。

```
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
```

狀態行檢查 — 該命令允許使用者指定正規表示式的清單，以便與響應的狀態行相匹配。允許或重置操作可應用於符合類對映條件的請求或響應。新增日誌操作會導致系統日誌消息：

```
APPFW-6-HTTP_STLINE_REGEX_MATCHED
```

命令用法：

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

用例示例

配置http appfw以在每次嘗試訪問禁止的頁面時記錄警報。被禁止的頁面通常包含403狀態代碼，並且狀態行看起來像`HTTP/1.0 403\r\n`。

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

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

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

- Content-type inspection — 此命令驗證消息報頭的content-type是否在支援的內容型別清單中。它還驗證標頭的content-type是否與消息資料或實體正文部分的內容匹配。如果配置了關鍵字不匹配，該命令將根據請求消息的接受欄位值驗證響應消息的content-type。允許或重置操作可應用於符合類對映條件的請求或響應。新增日誌操作會導致相應的系統日誌消息：

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

命令用法：

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

用例示例配置http appfw策略以阻止承載具有未知內容型別的請求和響應的http會話。

```
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
```

埠誤用檢查 — 此命令用於防止http埠(80)被誤用於其他應用程式，如IM、P2P、隧道等。允許或重置操作可應用於符合類對映條件的請求或響應。新增日誌操作會導致相應的系統日誌消息：

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

命令用法：

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

用例示例

配置http appfw策略以阻止為IM應用程式誤用的http會話。

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

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

- Strict-http inspection — 此命令可對HTTP請求和響應啟用嚴格的協定一致性檢查。允許或重置操作可應用於符合類對映條件的請求或響應。新增日誌操作會導致系統日誌消息：

  ```
  APPFW-4- HTTP_PROTOCOL_VIOLATION
  ```

  命令用法：

  ```
  match req-resp protocol-violation
  ```

  用例示例配置http appfw策略以阻止違反RFC 2616的請求或響應：

  ```
  class-map type inspect http proto-viol_cm
     match req-resp protocol-violation

  policy-map type inspect http proto-viol_pm
     class type inspect http proto-viol_cm
        reset
  ```

- Transfer-Encoding Inspection — 此命令提供允許、拒絕或監控其傳輸編碼型別與已配置型別相匹配的請求/響應的功能。允許或重置操作可應用於符合類對映條件的請求或響應。新增日誌操作會導致系統日誌消息：

  ```
  APPFW-6- HTTP_TRANSFER_ENCODING
  ```

  命令用法：

  ```
  match {request|response|req-resp} header transfer-encoding
  {regex <parameter-map-name> |gzip|deflate|chunked|identity|all}
  ```

  用例示例配置http appfw策略以阻止具有壓縮型別編碼的請求或響應。

  ```
  class-map type inspect http trans_encoding_cm
     match req-resp header transfer-encoding type compress

  policy-map type inspect http trans_encoding_pm
     class type inspect http trans_encoding_cm
        reset
  ```

- Java Applet檢測 — 此命令檢查響應是否具有Java applet，並在檢測到applet時應用配置的操作。允許或重置操作可應用於符合類對映條件的請求或響應。新增日誌操作會導致系統日誌消息：

  ```
  APPFW-4- HTTP_JAVA_APPLET
  ```

  命令用法：

  ```
  match response body java-applet
  ```

  用例示例配置http appfw策略以阻止java applet。

  ```
  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
  ```

適用於即時通訊和對等應用控制的ZFW支援

Cisco IOS軟體版本12.4(9)T引入了適用於IM和P2P應用的ZFW支援。

Cisco IOS軟體最初在Cisco IOS軟體版本12.4(4)T中為IM應用控制提供支援。ZFW的初始版本不支援ZFW介面中的IM應用程式。如果需要IM應用控制，則使用者無法遷移到ZFW配置介面。Cisco IOS軟體版本12.4(9)T引入了對IM檢查的ZFW支援，支援Yahoo!Messenger(YM)、MSN Messenger(MSN)和AOL Instant Messenger(AIM)。Cisco IOS軟體版本12.4(9)T是Cisco IOS軟體的第一個版本，為P2P檔案共用應用程式提供本地Cisco IOS防火牆支援。

IM和P2P檢測都為應用流量提供第4層和第7層策略。這意味著ZFW可以提供允許或拒絕流量的基本狀態檢測，以及對各種協定中的特定活動進行精細的第7層控制，從而允許某些應用活動而拒絕其他應用活動。

P2P應用檢測和控制

SDM 2.2在其防火牆配置部分引入了P2P應用程式控制。SDM應用了基於網路的應用識別(NBAR)和QoS策略來檢測並管制P2P應用活動，使其線路速率為零，並阻止所有P2P流量。這就引出了這樣一個問題：CLI使用者（Cisco IOS防火牆CLI中預期的P2P支援）無法在CLI中配置P2P阻止，除非他們知道必要的NBAR/QoS配置。Cisco IOS軟體版本12.4(9)T在ZFW CLI中引入了原生P2P控制，以利用NBAR檢測P2P應用活動。此軟體版本支援多種P2P應用協定：

- BitTorrent
- 驢子
- FastTrack
- 格努特拉
- KaZaA / KaZaA2
- WinMX

由於「埠跳躍」行為和其他避免檢測的技巧，以及頻繁更改和更新修改協定行為的P2P應用所引起的問題，P2P應用尤其難以檢測。ZFW將本地防火牆狀態檢測與NBAR的流量識別功能相結合，在ZFW的CPL配置介面中提供P2P應用控制。NBAR提供兩個卓越的優勢：

- 可選的基於啟發式的應用程式識別，用於識別存在複雜且難以檢測行為的應用程式
- 可擴展的基礎設施，它提供更新機制，可及時瞭解協定更新和修改

配置P2P檢測

如前所述，P2P檢測和控制提供第4層狀態檢測和第7層應用控制。如果本地應用服務埠檢查充分，則第4層檢查的配置與其他應用服務類似：

```
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]
```

請注意match protocol [service-name]中的其他簽名選項。當在match protocol語句末尾新增簽名選項時，NBAR啟發式應用於流量，以搜尋指示特定P2P應用活動的流量中的通告。這包括埠跳變和應用程式行為的其他更改，以避免流量檢測。這種級別的流量檢測是以提高CPU利用率和降低網路吞吐量能力為代價的。如果未應用簽名選項，則不會應用基於NBAR的啟發式分析來檢測埠跳變行為，並且不會對CPU利用率產生相同程度的影響。

本地服務檢查的缺點是：如果應用程式跳轉到非標準源和目標埠，或者如果應用程式更新為開始對無法識別的埠號執行操作，則無法保持對P2P應用程式的控制：

應用程式 本地埠(由12.4(15)T PAM清單識別)
bittorrent TCP 6881-6889
edonkey TCP 4662
fasttrack TCP 1214
格努特拉 TCP 6346-6349 TCP 6355,5634 UDP 6346-6348
kazaa2 取決於PAM
winmx TCP 6699

如果要允許（檢查）P2P流量，可能需要提供其他配置。某些應用程式可以使用多個P2P網路，或者實施在防火牆配置中需要支援的特定行為，以允許應用程式工作：

- BitTorrent客戶端通常通過運行在某些非標準埠上的http與「跟蹤器」（對等目錄伺服器）通訊。這通常是TCP 6969，但您可能需要檢查Torrent特定的跟蹤器埠。如果您希望允許BitTorrent，容納額外埠的最佳方法是將HTTP配置為匹配協定之一，並使用ip port-map命令將TCP 6969新增到HTTP:
  ```
  ip port-map http port tcp 6969
  ```
  您需要將http和bittorrent定義為應用於類對映的匹配條件。
- eDonkey似乎會啟動同時檢測為eDonkey和Gnutella的連線。
- KaZaA檢測完全依賴於NBAR簽名檢測。

第7層（應用）檢測增強了第4層檢測的功能，可識別並應用特定於服務的操作，如有選擇地阻止或允許檔案搜尋、檔案傳輸和文本聊天功能。特定於服務的功能因服務而異。

P2P應用檢測與HTTP應用檢測類似：

```
!configure the layer-7 traffic characteristics:
class-map type inspect [p2p protocol] match-any p2p-l7-cmap
 match action
!
!configure the action to be applied to the traffic
!matching the specific characteristics:
policy-map type inspect [p2p protocol] p2p-l7-pmap
 class type inspect p2p p2p-l7-cmap
  [ reset | allow ]
```

```
  log
!
!define the layer-4 inspection policy
class-map type inspect match-all p2p-l4-cmap
 match protocol [p2p protocol]
!
!associate layer-4 class and layer-7 policy-map
!in the layer-4 policy-map:
policy-map type inspect private-allowed-policy
 class type inspect p2p-l4-cmap
  [ inspect | drop | pass ]
  service-policy p2p p2p-l7-pmap
```

P2P應用檢測為第4層檢測所支援的應用子集提供特定於應用的功能：

- edonkey
- fasttrack
- 格努特拉
- kazaa2

這些應用程式中的每一個都提供特定於應用程式的匹配條件選項：

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
```

格努特拉

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

kazaa2

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

新的P2P協定定義或對當前P2P協定的更新可以通過NBAR的動態pdlm更新功能進行載入。以下是載入新PDLM的組態命令：

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

新的協定可用於類型別inspect的match protocol命令。如果新的P2P協定包含服務（子協定），新

的第7層inspect類對映型別以及第7層匹配條件將可用。

IM應用檢測和控制

Cisco IOS軟體版本12.4(4)T引入IM應用程式偵測與控制。12.4(6)T中沒有在ZFW中引入IM支援，因此使用者無法在相同的防火牆策略中應用IM控制和ZFW，因為ZFW和舊式防火牆功能不能在給定介面上共存。

Cisco IOS軟體版本12.4(9)T支援對以下IM服務的狀態檢測和應用控制：

- AOL即時通訊工具
- MSN Messenger
- 雅虎！Messenger

IM檢查與大多數服務略有不同，因為IM檢查控制對每個給定服務對特定主機組的訪問。IM服務通常依賴於相對永久的一組目錄伺服器，客戶端必須能夠聯絡這些目錄伺服器才能訪問IM服務。從協定或服務的角度來看，IM應用往往很難控制。控制這些應用程式的最有效方法是限制對固定IM伺服器的訪問。

配置IM檢測

IM檢測和控制都提供第4層狀態檢測

和第7層應用控制。

第4層檢查的配置類似於其他應用服務：

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

IM應用程式可以聯絡其多個埠上的伺服器以維護其功能。要允許具有檢查操作的給定IM服務，您不需要伺服器清單來定義允許訪問IM服務的伺服器。但是，當您配置指定給定IM服務（如AOL Instant Messenger）的類對映並在關聯的策略對映中應用丟棄操作時，可能會導致IM客戶端嘗試並找到允許連線到Internet的不同埠。如果您不想允許連線到給定服務，或者希望將IM服務功能限製為文本聊天，則必須定義伺服器清單，以便ZFW可以識別與IM應用關聯的流量：

```
!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
```

例如，Yahoo IM伺服器清單的定義如下：

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

您需要將伺服器清單應用於協定定義：

```
class-map type inspect match-any ym-l4-cmap
 match protocol ymsgr ymsgr-pmap
```
您必須配置ip domain lookup和ip name-server ip.ad.re.ss命令才能啟用名稱解析。

IM伺服器名稱是相當動態的。您需要定期檢查已配置的IM伺服器清單是否完整正確。

第7層（應用）檢測增強了第4層檢測的功能，可識別並應用特定於服務的操作，如選擇性地阻止或允許文本聊天功能，以及拒絕其他服務功能。

IM Application Inspection目前能夠區分文本聊天活動和所有其他應用服務。為了將IM活動限製為文本聊天，請配置第7層策略：

```
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]
```
將第7層策略應用於Yahoo!之前配置的Messenger策略：

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

ZFW提供URL過濾功能，將對Web內容的訪問限製為路由器上定義的白名單或黑名單所指定的內容，或者將域名轉發到URL過濾伺服器以驗證對特定域的訪問。Cisco IOS軟體版本12.4(6)T到12.4(15)T中的ZFW URL過濾是作為額外的原則動作而套用，與應用檢查類似。

對於基於伺服器的URL過濾，必須定義描述urlfilter伺服器配置的引數對映：

```
parameter-map type urlfilter websense-parmap
 server vendor [n2h2 | websense] 10.1.1.1
```
如果優先使用靜態白名單或黑名單，您可以定義特別允許或拒絕的域或子域的清單，而反向操作將應用於與清單不匹配的流量：

```
parameter-map type urlfilter websense-parmap
 exclusive-domain deny .disallowed.com
 exclusive-domain permit .cisco.com
```
如果在獨佔域定義中使用拒絕選項定義URL黑名單，則允許所有其他域。如果定義了任何「允許」

定義，則必須明確指定允許的所有域，類似於IP訪問控制清單的功能。

設定與HTTP流量匹配的類對映：

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

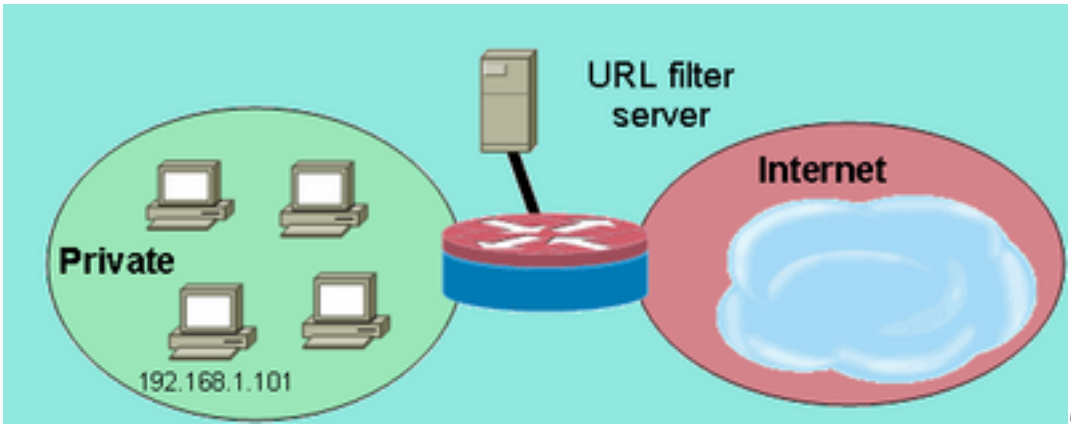
定義將類對映與inspect和urlfilter操作關聯的策略對映：

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

這將配置與URL過濾伺服器通訊的最低要求。有多個選項可用於定義其他URL過濾行為。

某些網路部署希望對部分主機或子網應用URL過濾，而對其他主機繞過URL過濾。例如，在圖9中，私有區域中的所有主機都必須由URL過濾伺服器檢查HTTP流量，特定主機192.168.1.101除外。

圖10:URL過濾示例拓撲



URL過濾示例拓撲

如果定義兩個不同的類對映可以完成此操作：

- 一個類對映，僅匹配接收URL過濾的較大主機組的HTTP流量。
- 一個類對映用於不接收URL過濾的較小主機組。第二個類對映匹配HTTP流量以及免除URL過濾策略的主機清單。

兩個類對映均在策略對映中配置，但只有一個類對映接收urlfilter操作：

```
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
```

控制對路由器的訪問

如果大多數網路安全工程師將路由器的管理介面（例如，SSH、Telnet、HTTP、HTTPS、SNMP等）暴露到公共Internet，則他們感到不舒服。在特定情況下，還需要對路由器的LAN訪問進行控制。Cisco IOS軟體提供許多選項來限制對各種介面的存取，包括網路基礎保護(NFP)功能系列、適用於管理介面的各種存取控制機制，以及ZFW的自區域網路。您必須檢查其他功能，例如VTY訪問控制、管理平面保護和SNMP訪問控制，以確定路由器控制功能的哪個組合最適合您的特定應用。

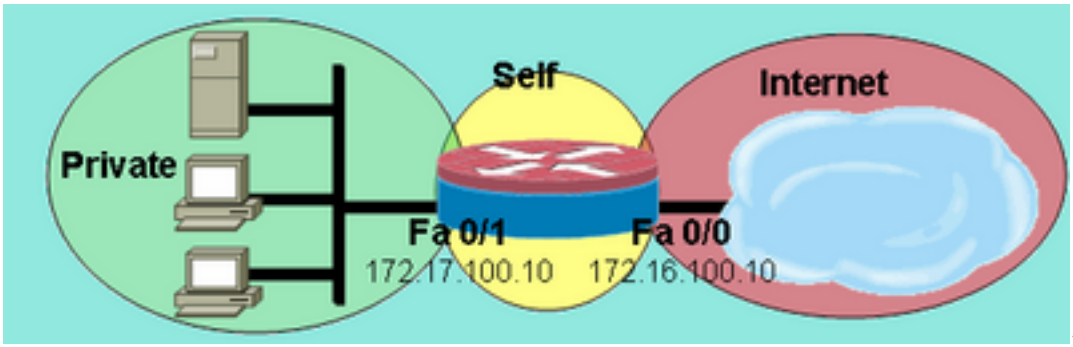
一般來說，NFP功能系列最適合於控制發往路由器本身的流量。請參閱Cisco IOS軟體中的控制平面安全概述以瞭解有關使用NFP功能保護路由器的資訊。

如果您決定應用ZFW來控制進出路由器本身IP地址的流量，您必須瞭解防火牆的預設策略和功能不同於可用於傳輸流量的策略和功能。中轉流量定義為來源和目的地IP位址與應用於任何路由器介面的任何IP位址不匹配的網路流量，並且該流量不會導致路由器傳送網路控制訊息，例如ICMP TTL到期或網路/主機無法到達訊息。

ZFW對區域之間移動的流量應用預設的deny-all策略，但如常規規則所述，隱式允許直接流向路由器介面地址的任何區域中的流量。這可確保將區域防火牆配置應用到路由器時，保持與路由器管理介面的連線。如果同一個deny-all策略影響直接到路由器的連線，則必須在路由器上配置區域之前應用完整的管理策略配置。如果策略實施不當或應用順序錯誤，這可能會中斷管理連線。

當介面配置為區域成員時，連線到介面的主機將包括在區域中。但是，進出路由器介面IP地址的流量不受區域策略控制（圖10的說明中所述的情況除外）。 而是當配置ZFW時，路由器上的所有IP介面會自動成為自分割槽的一部分。為了控制從路由器上的不同區域移動到路由器介面的IP流量，必須應用策略來阻止或允許/檢查區域與路由器自區域之間的流量，反之亦然（請參見圖11）。

圖11:在網路區域和路由器自身區域之間應用策略



在網路區域和路由器自身區域之間應用策略

雖然路由器在所有區域和自區域之間提供預設允許策略，但如果從任何區域向自區域配置策略，並且沒有從自區域向路由器的使用者可配置的介面連線區域配置策略，則所有源自路由器的流量在返迴路由器時都會遇到connected-zone to self-zone策略並被阻止。因此，必須檢查源自路由器的流量，以允許其返回自區域。

> **附註**：Cisco IOS軟體一律使用與介面「最接近」目的地主機關聯的IP位址來傳輸流量，例如系統日誌、tftp、telnet和其他控制平面服務，並使此流量遵循自區域防火牆原則。但是，如果服務使用包括但不限於logging source-interface [type number] 、 ip tftp source-interface [type number]和ip telnet source-interface [type number]等命令將特定介面定義為source-interface，則該流量會受到自區域的影響。

> **注意**：某些服務（尤其是路由器的IP語音服務）使用臨時或不可配置的介面，不能將其分配給

安全區域。如果這些服務的流量無法與已配置的安全區域相關聯，則這些服務無法正常工作。

自區域策略限制

與傳輸流量區域對可用的策略相比，自區域策略的功能有限：

- 與經典的有狀態檢測一樣，路由器生成的流量限於H.323的TCP、UDP、ICMP和複雜協定檢測。
- 「應用程式檢查」不可用於自區域策略。
- 不能在自區域策略上配置會話和速率限制。

自區域策略配置

在大多數情況下，以下是路由器管理服務的理想訪問策略：

- 拒絕所有Telnet連線，因為Telnet的明文協定很容易暴露使用者憑證和其他敏感資訊。
- 允許來自任何區域中任何使用者的SSH連線。SSH會加密使用者憑證和作業階段資料，提供保護，防止惡意使用者利用封包擷取工具窺探使用者活動，並危及使用者憑證或路由器組態等敏感資訊。SSH版本2提供更強大的保護，並解決SSH版本1固有的特定漏洞。
- 如果專用區域可信，則允許從專用區域到路由器的HTTP連線。否則，如果私有區域可能使惡意使用者危害資訊，HTTP不會使用加密來保護管理流量，並且可能會洩露敏感資訊，如使用者憑證或配置。
- 允許來自任何區域的HTTPS連線。與SSH類似，HTTPS會加密會話資料和使用者憑證。
- 限制對特定主機或子網的SNMP訪問。SNMP可用於修改路由器配置和顯示配置資訊。SNMP必須在各種團體上配置訪問控制。
- 阻止從公共Internet到專用區域地址的ICMP請求（假設專用區域地址是可路由的）。 如有必要，可以為ICMP流量暴露一個或多個公有地址以進行網路故障排除。有幾種ICMP攻擊可用於耗盡路由器資源或通告網路拓撲和架構。

路由器可以應用此類策略，為必須控制的每個區域新增兩個區域對。傳入或傳出路由器自帶區域的流量的每個區域對都必須由相反方向的相應策略匹配，除非流量不是源自相反方向。可以應用一個策略對映，每個策略對映用於入站和出站區域對，用於描述所有流量，也可以應用每個區域對的特定策略對映。每個策略對映的特定區域對配置提供了檢視與每個策略對映匹配的活動所需的粒度。

以SNMP管理站172.17.100.11和TFTP伺服器172.17.100.17為例，此輸出提供了整個管理介面訪問策略的示例：

```
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
```

很遺憾，自區域策略不能檢查TFTP傳輸。因此，如果TFTP必須經過防火牆，則防火牆必須將所有流量傳入TFTP伺服器或從TFTP伺服器傳出。

如果路由器終止IPSec VPN連線，您還必須定義策略以通過IPSec ESP、IPSec AH、ISAKMP和NAT-T IPSec(UDP 4500)。 這取決於根據您使用的服務需要哪些服務。除上述策略外，還可以應用下一個策略。注意對策略對映的更改，其中VPN流量的類對映已插入通過操作。通常，加密流量是可信的，除非安全策略規定必須允許進出指定終端的加密流量。

```
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
```

區域防火牆和廣域應用程式服務

有關提供配置示例和使用指南的應用程式說明，請參閱思科廣域應用服務（軟體版本4.0.13）— 軟體版本4.0.13的新功能版本說明

使用show和debug命令監控基於區域的策略防火牆

ZFW引入了新命令來檢視策略配置和監控防火牆活動。

顯示區域說明和指定區域中包含的介面：

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

如果未包含區域名稱，命令將顯示所有已配置區域的資訊。

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

顯示連線到區域對的源區域、目標區域和策略：

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

未指定源或目標時，將顯示包含源、目標和相關策略的所有區域對。如果只提到源/目標區域，則會顯示包含此區域作為源/目標的所有區域對。

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

顯示指定的策略對映：

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

如果未指定策略對映的名稱，則它顯示型別為inspect的所有策略對映（以及包含子型別的第7層策略對映）。

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

顯示指定區域對上的運行時檢查型別策略對映統計資訊。

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

如果未提及區域對名稱，則顯示所有區域對上的策略對映。

sessions選項顯示由策略對映應用程式在指定區域對上建立的檢查會話。

```
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
```

urlfilter關鍵字顯示與指定的策略對映相關的urlfilter相關統計資訊（如果未指定區域對名稱，則顯示所有目標上的策略對映）：

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

當同時指定cache關鍵字和urlfilter時，它會顯示urlfilter cache（屬於IP地址）。

用於inspect policy-maps的show policy-map命令摘要：

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

調整基於區域的策略防火牆拒絕服務保護

ZFW提供DoS保護，以提醒網路工程師注意網路活動的劇烈變化，並緩解有害活動，從而降低網路活動變化的影響。ZFW為每個策略對映的類對映維護單獨的計數器。因此，如果將一個類對映用於兩個不同區域對的策略對映，則會應用兩組不同的DoS保護計數器。

ZFW在12.4(11)T之前的Cisco IOS軟體版本中將DoS攻擊緩解作為預設選項。預設DoS保護行為隨Cisco IOS軟體版本12.4(11)T而更改。

有關TCP SYN DoS攻擊的詳細資訊，請參閱定義防禦TCP SYN拒絕服務攻擊的策略。

附錄

附錄 A：基本配置

```
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
```

附錄 B：最終（完成）配置

```
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
```

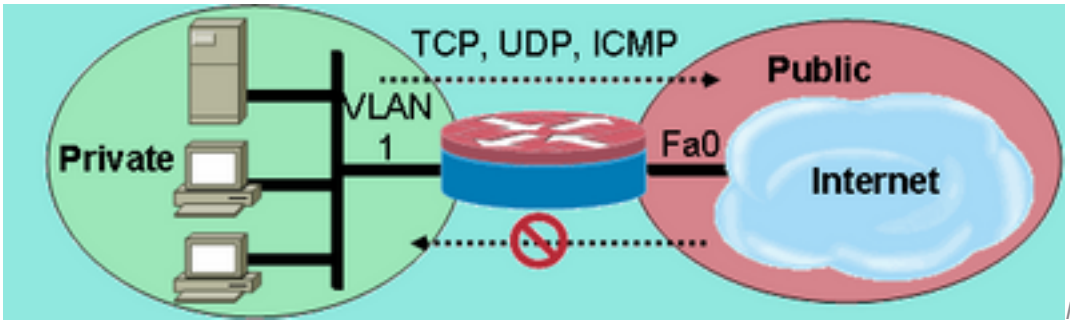
```
 class type inspect Xwindows-class
  inspect
policy-map type inspect private-internet-policy
  class type inspect internet-traffic-class
   inspect
  class type inspect bad-http-class
   drop
!
zone security clients
zone security servers
zone security private
zone security internet
zone security 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
```

附錄 C：兩個區域的基本區域策略防火牆配置

此示例提供簡單的配置，作為測試Cisco IOS軟體ZFW增強功能的基礎。此配置是1811路由器上配置的兩個區域的型號配置。專用區域應用於路由器的固定交換機埠，因此交換機埠上的所有主機都連線到VLAN 1。公共區域應用在FastEthernet 0上（請參見圖12）。

圖12:FastEthernet 0上應用的公共區域



FastEthernet 0上應用的公共區域

```
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
```

相關資訊

- 技術支援與文件 - Cisco Systems

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。