Informazioni sulla progettazione del firewall per i criteri basati sulle aree

Sommario

Introduzione

Questo documento descrive il modello di configurazione per il set di funzionalità di Cisco IOS® Firewall, Zone-based Policy Firewall (ZFW).

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Premesse

Questo nuovo modello di configurazione offre criteri intuitivi per router con più interfacce, una maggiore granularità dell'applicazione dei criteri firewall e un criterio di negazione totale predefinito che impedisce il traffico tra le aree di sicurezza del firewall fino a quando non viene applicato un

criterio esplicito per consentire il traffico desiderato.

Quasi tutte le funzionalità classiche di Cisco IOS Firewall implementate prima del software Cisco IOS versione 12.4(6)T sono supportate nella nuova interfaccia di ispezione delle policy basata su zone:

- Ispezione pacchetti stateful
- Cisco IOS Firewall con riconoscimento VRF
- Filtro URL
- Attenuazione DoS (Denial-of-Service)

Dal software Cisco IOS versione 12.4(9)T, è stato aggiunto il supporto ZFW per i limiti di sessione/connessione e velocità di trasmissione per classe, oltre a ispezione e controllo delle applicazioni:

- HTTP
- Protocollo POP3 (Post Office Protocol), protocollo IMAP (Internet Mail Access Protocol), protocollo SMTP/ESMTP (Simple Mail Transfer Protocol/Enhanced Simple Mail Transfer Protocol)
- RPC (Sun Remote Procedure Call)
- Applicazioni di messaggistica immediata:Microsoft MessengerYahoo! MessengerAOL Instant Messenger
- Condivisione file peer-to-peer (P2P):BittorrentKaZaAGnutellaeDonkey

Dal software Cisco IOS versione 12.4(11)T sono state aggiunte statistiche per semplificare il tuning della protezione DoS.

Alcune funzionalità e funzionalità di Cisco IOS Classic Firewall non sono ancora supportate in uno ZFW nel software Cisco IOS versione 12.4(15)T:

- Proxy di autenticazione
- Failover stateful del firewall
- MIB firewall unificato
- Ispezione stateful IPv6
- Supporto TCP non in ordine

ZFW in genere migliora le prestazioni di Cisco IOS per la maggior parte delle attività di ispezione dei firewall. Né Cisco IOS ZFW né il firewall classico includono il supporto dell'ispezione con stato per il traffico multicast.

Panoramica dei criteri basati sulle zone

L'ispezione con stato di Cisco IOS Classic Firewall (in precedenza nota come Controllo degli accessi basato sul contesto o CBAC) impiegava un modello di configurazione basato sull'interfaccia, in cui a un'interfaccia era applicato un criterio di ispezione con stato. Tutto il traffico che passa attraverso quell'interfaccia ha ricevuto la stessa policy di ispezione. Questo modello di configurazione ha limitato la granularità dei criteri firewall e ha causato confusione nella corretta applicazione dei criteri firewall, in particolare negli scenari in cui i criteri firewall devono essere applicati tra più interfacce.

Il firewall di policy basato su zone (noto anche come ZFW, Zone-Policy Firewall) modifica la configurazione del firewall dal precedente modello basato su interfacce a un modello basato su

zone più flessibile e di più facile comprensione. Le interfacce vengono assegnate alle zone e i criteri di ispezione vengono applicati al traffico che si sposta tra le zone. Le policy interzona offrono notevole flessibilità e granularità, pertanto è possibile applicare policy di ispezione diverse a più gruppi host collegati alla stessa interfaccia router.

I criteri firewall vengono configurati con Cisco Policy Language (CPL), che utilizza una struttura gerarchica per definire l'ispezione per i protocolli di rete e i gruppi di host a cui può essere applicata l'ispezione.

Modello di configurazione dei criteri basati su zone

ZFW modifica completamente il modo in cui si configura un'ispezione di Cisco IOS Firewall, rispetto a Cisco IOS Classic Firewall.

La prima modifica di rilievo apportata alla configurazione del firewall è l'introduzione della configurazione basata su zone. Cisco IOS Firewall è la prima funzione di difesa dalle minacce del software Cisco IOS ad implementare un modello di configurazione delle zone. Altre feature possono adottare il modello di zona nel tempo. Il modello di configurazione basata sull'interfaccia CBAC (Cisco IOS Classic Firewall Stateful Inspection) che utilizza il set di comandi ip inspect viene mantenuto per un determinato periodo di tempo. Tuttavia, poche, se presenti, nuove funzionalità sono configurabili con la CLI (Command-Line Interface) classica. ZFW non utilizza i comandi di ispezione con stato o CBAC. I due modelli di configurazione possono essere utilizzati contemporaneamente sui router, ma non sulle interfacce. Non è possibile configurare un'interfaccia come membro dell'area di sicurezza e allo stesso tempo configurarla per ip inspect.

Le zone definiscono i bordi di protezione della rete. Una zona definisce un limite in cui il traffico è soggetto a restrizioni dei criteri mentre attraversa un'altra area della rete. Il criterio predefinito ZFW tra le zone è deny all. Se non viene configurato alcun criterio in modo esplicito, tutto il traffico che si sposta tra le zone verrà bloccato. Si tratta di una deviazione significativa dal modello di ispezione con conservazione dello stato, in cui il traffico era implicitamente consentito fino al blocco esplicito con un Access Control List (ACL).

La seconda modifica di rilievo è l'introduzione di un nuovo linguaggio dei criteri di configurazione noto come CPL. Gli utenti che conoscono MQC (Modular quality-of-service) del software Cisco IOS possono riconoscere che il formato è simile all'uso QoS delle mappe di classe per specificare il traffico interessato dall'azione applicata in una mappa dei criteri.

Regole Per L'Applicazione Policy Firewall Basata Su Zone

L'appartenenza dell'interfaccia di rete del router alle zone è soggetta a diverse regole che determinano il comportamento dell'interfaccia, così come il traffico che si sposta tra le interfacce dei membri della zona:

- Ènecessario configurare una zona prima di poter assegnare le interfacce alla zona.
- Un'interfaccia può essere assegnata a una sola area di sicurezza.
- Tutto il traffico da e verso una determinata interfaccia viene bloccato in modo implicito quando l'interfaccia viene assegnata a una zona, ad eccezione del traffico da e verso altre interfacce della stessa zona e del traffico verso qualsiasi interfaccia del router.
- Per impostazione predefinita, il traffico viene consentito in modo implicito tra le interfacce che sono membri della stessa zona.

- Per autorizzare il traffico da e verso l'interfaccia di un membro della zona, è necessario configurare una policy che consenta o controlli il traffico tra la zona e qualsiasi altra zona.
- L'area autonoma è l'unica eccezione al criterio di negazione di tutti i valori predefinito. Tutto il traffico diretto a qualsiasi interfaccia del router è consentito fino a quando non viene esplicitamente negato.
- Il traffico non può passare tra un'interfaccia del membro di una zona e un'interfaccia che non è un membro della zona. Le azioni di superamento, controllo e rilascio possono essere applicate solo tra due zone.
- Le interfacce che non sono state assegnate a una zona funzionano come porte di router classiche e possono ancora utilizzare la configurazione classica con ispezione stateful/CBAC.
- Se è necessario che un'interfaccia sulla scatola non faccia parte dei criteri zona/firewall. Può comunque essere necessario inserire l'interfaccia in una zona e configurare un criterio pass all (una sorta di criterio fittizio) tra la zona e qualsiasi altra zona a cui si desidera indirizzare il flusso di traffico.
- Dal comportamento precedente, se il traffico deve fluire tra tutte le interfacce di un router, tutte le interfacce devono appartenere al modello di zoning (ogni interfaccia deve essere un membro di una zona o di un'altra).
- L'unica eccezione al comportamento precedente, ossia l'approccio Deny by default (Nega per impostazione predefinita), è il traffico da e verso il router, che è autorizzato per impostazione predefinita. È possibile configurare un criterio esplicito per limitare tale traffico.

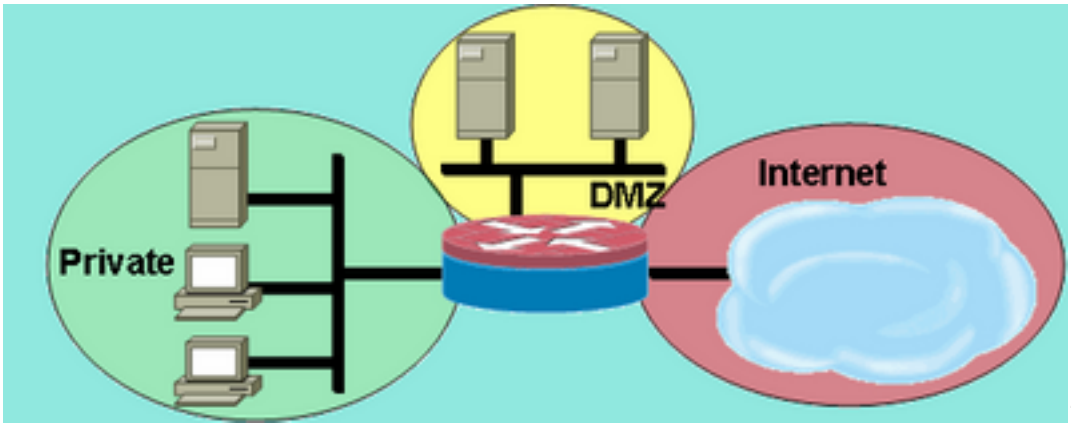
Progettazione della sicurezza di rete dei criteri basati sulle aree

Ènecessario configurare un'area di protezione per ogni area di protezione relativa all'interno della rete, in modo che tutte le interfacce assegnate alla stessa area siano protette con un livello di protezione simile. Ad esempio, si consideri un router di accesso con tre interfacce:

- Un'interfaccia connessa alla rete Internet pubblica
- Un'interfaccia connessa a una LAN privata che non deve essere accessibile da Internet pubblica
- Un'interfaccia connessa a una zona demilitarizzata di servizi Internet (DMZ), in cui un server Web, un server DNS (Domain Name System) e un server di posta elettronica devono essere accessibili al pubblico Internet

Ogni interfaccia di questa rete è assegnata alla propria zona, sebbene si possa consentire l'accesso variabile da Internet pubblica a host specifici nella DMZ e vari criteri di utilizzo delle applicazioni per gli host nella LAN protetta (vedere Figura 1).

Figura 1: Topologia area di sicurezza di base



Topologia area di sicurezza di base

In questo esempio, ogni zona contiene una sola interfaccia. Se si aggiunge un'interfaccia aggiuntiva alla zona privata, gli host connessi alla nuova interfaccia della zona possono trasmettere il traffico a tutti gli host sull'interfaccia corrente della stessa zona. Inoltre, il traffico degli host verso gli host di altre zone è influenzato in modo simile dalle policy correnti.

In genere, la rete di esempio dispone di tre criteri principali:

- Connessione a Internet da zona privata
- Connettività zona privata a host DMZ
- Connettività dell'area Internet agli host DMZ

Poiché la zona demilitarizzata è esposta alla rete pubblica Internet, gli host della zona possono essere soggetti ad attività indesiderate da parte di utenti malintenzionati che possono riuscire a danneggiare uno o più host della zona demilitarizzata. Se non viene fornito alcun criterio di accesso per consentire agli host della zona DMZ di raggiungere gli host della zona privata o gli host della zona Internet, gli utenti che hanno compromesso gli host della zona DMZ non possono utilizzare gli host della zona DMZ per effettuare ulteriori attacchi contro gli host privati o Internet. ZFW impone una postura di sicurezza predefinita proibitiva. Pertanto, a meno che agli host DMZ non venga specificamente fornito l'accesso ad altre reti, le altre reti sono protette da qualsiasi connessione dagli host DMZ. Analogamente, gli host Internet non dispongono dell'accesso agli host della zona privata, pertanto gli host della zona privata sono al sicuro da accessi indesiderati da parte degli host Internet.

Usa VPN IPSec con firewall dei criteri basato su zone

I recenti miglioramenti apportati alla VPN IPSec semplificano la configurazione dei criteri firewall per la connettività VPN. Le interfacce VTI (Virtual Tunnel Interface) IPSec e GRE+IPSec consentono di limitare le connessioni VPN da sito a sito e client a un'area di sicurezza specifica posizionando le interfacce tunnel in un'area di sicurezza specifica. Le connessioni possono essere isolate in una DMZ VPN se la connettività deve essere limitata da un criterio specifico. Oppure, se la connettività VPN è implicitamente attendibile, è possibile posizionare la connettività VPN nella stessa area di sicurezza della rete interna attendibile.

Se viene applicato un IPSec non VTI, i criteri firewall per la connettività VPN richiedono un esame approfondito per mantenere la protezione. I criteri di zona devono consentire in modo specifico l'accesso tramite un indirizzo IP per gli host di siti remoti o i client VPN se gli host sicuri si trovano in una zona diversa da quella della connessione crittografata del client VPN al router. Se il criterio di accesso non è configurato correttamente, gli host da proteggere possono essere esposti a host indesiderati e potenzialmente ostili. Per ulteriori informazioni sui concetti e sulla configurazione, fare riferimento a Utilizzo di VPN con Policy Firewall basato su zone.

Configurazione di Cisco Policy Language (CPL)

Questa procedura può essere utilizzata per configurare un ZFW. La sequenza dei passaggi non è importante, ma alcuni eventi devono essere completati in modo corretto. Ad esempio, è necessario configurare una mappa delle classi prima di assegnare una mappa delle classi a una mappa dei criteri. Analogamente, non è possibile assegnare una mappa dei criteri a una coppia di zone fino a quando il criterio non è stato configurato. Se si tenta di configurare una sezione che si basa su un'altra parte della configurazione non configurata, il router risponde con un messaggio di errore.

1. Definire le zone.
2. Definite le coppie di zone.
3. Definire mappe di classi che descrivono il traffico a cui devono essere applicati criteri mentre attraversa una coppia di zone.
4. Definire le mappe delle regole per applicare un'azione al traffico delle mappe delle classi.
5. Applicare mappe di criteri a coppie di zone.
6. Assegnare le interfacce alle zone.

Configura mapping di classi del firewall per i criteri basati su zone

Le mappe di classe definiscono il traffico selezionato dal firewall per l'applicazione dei criteri. Le mappe di classe di layer 4 ordinano il traffico in base ai criteri elencati di seguito. Questi criteri vengono specificati con il comando match in una mappa delle classi:

- Access-group: un ACL standard, esteso o denominato può filtrare il traffico in base all'indirizzo IP di origine e di destinazione e alla porta di origine e di destinazione.
- Protocollo: i protocolli di layer 4 (TCP, UDP e ICMP) e i servizi applicativi quali HTTP, SMTP, DNS e così via. È possibile specificare qualsiasi servizio conosciuto o definito dall'utente noto a Port-Application Mapping.
- Class-map: una class-map subordinata che fornisce criteri di corrispondenza aggiuntivi può essere nidificata all'interno di un'altra class-map.
- Not - Il criterio not specifica che qualsiasi traffico che non corrisponde a un servizio specificato (protocollo), a un gruppo di accesso o a una mappa di classe subordinata è selezionato per la mappa di classe.

Combina criteri di corrispondenza: "Match-Any" e "Match-All"

Le mappe di classi possono applicare operatori di corrispondenza qualsiasi o di corrispondenza totale per determinare come applicare i criteri di corrispondenza. Se si specifica match-any, il traffico deve soddisfare solo uno dei criteri di corrispondenza nella class-map. Se si specifica match-all, il traffico deve corrispondere a tutti i criteri della mappa di classe per appartenere a quella particolare classe.

I criteri di corrispondenza devono essere applicati in ordine da più specifico a meno specifico se il traffico soddisfa più criteri. Si consideri, ad esempio, la seguente mappa delle classi:

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

```
 match protocol tcp
```

Il traffico HTTP deve prima incontrare il protocollo di corrispondenza http per assicurarsi che venga gestito dalle funzionalità specifiche del servizio dell'ispezione HTTP. Se le righe di corrispondenza sono invertite, quindi il traffico incontra l'istruzione TCP del protocollo di corrispondenza prima di confrontarla con il protocollo http, il traffico viene semplicemente classificato come traffico TCP e ispezionato in base alle funzionalità del componente Ispezione TCP del firewall. Questo è un problema per alcuni servizi come FTP, TFTP e diversi servizi multimediali e di segnalazione vocale come H.323, SIP, Skinny, RTSP e altri. Questi servizi richiedono capacità di ispezione aggiuntive per riconoscere le attività più complesse di questi servizi.

Applicazione di un ACL come criterio di corrispondenza

Le mappe di classi possono applicare un ACL come uno dei criteri di corrispondenza per l'applicazione dei criteri. Se una mappa delle classi corrisponde solo a un criterio, ovvero un ACL, e la mappa delle classi è associata a una mappa dei criteri che applica l'azione di ispezione, il router applica l'ispezione TCP o UDP di base a tutto il traffico consentito dall'ACL, ad eccezione del traffico che viene controllato con riconoscimento delle applicazioni da parte di ZFW. Sono inclusi (senza limitazioni) FTP, SIP, Skinny (SCCP), H.323, Sun RPC e TFTP. Se è disponibile l'ispezione specifica dell'applicazione e l'ACL consente il canale primario o di controllo, sono consentiti tutti i canali secondari o multimediali associati al canale primario/di controllo, indipendentemente dal fatto che l'ACL consenta o meno il traffico.

Se una mappa di classe applica solo ACL 101 come criterio di corrispondenza, viene visualizzato un ACL 101 come segue:

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

Tutto il traffico è autorizzato nella direzione dei criteri del servizio applicati a una determinata coppia di zone e il traffico di ritorno corrispondente a questa direzione è autorizzato nella direzione opposta. Pertanto, l'ACL deve applicare la restrizione per limitare il traffico a specifici tipi desiderati. Si noti che l'elenco PAM include servizi applicativi quali HTTP, NetBIOS, H.323 e DNS. Tuttavia, nonostante PAM sia a conoscenza dell'uso specifico di una determinata porta per quanto riguarda le applicazioni, il firewall applica solo una capacità specifica dell'applicazione sufficiente a soddisfare i ben noti requisiti del traffico delle applicazioni. Pertanto, il traffico delle applicazioni semplici, ad esempio telnet, SSH e altre applicazioni a canale singolo, vengono ispezionate come TCP e le relative statistiche vengono combinate nell'output del comando show. Se si desidera una visibilità specifica dell'applicazione per l'attività di rete, è necessario configurare l'ispezione dei servizi in base al nome dell'applicazione (configurare il protocollo di corrispondenza HTTP, il protocollo di corrispondenza Telnet e così via).

Confrontare le statistiche disponibili nell'output del comando show policy-map type inspect zone-pair da questa configurazione con i criteri firewall più espliciti mostrati più in basso nella pagina. Questa configurazione viene usata per ispezionare il traffico di un Cisco IP Phone e di diverse workstation che usano una varietà di traffico, tra cui 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
```

Questa configurazione è facile da definire e supporta tutto il traffico proveniente dalla zona privata (purché il traffico rispetti le porte di destinazione standard riconosciute da PAM), ma fornisce una visibilità limitata sull'attività di servizio e non offre l'opportunità di applicare i limiti di larghezza di banda e di sessione di ZFW per tipi di traffico specifici. Questo output del comando show policy-map type inspect zone-pair priv-pub è il risultato della precedente configurazione semplice che usa solo un'autorizzazione IP [subnet] o un ACL tra coppie di zone. Come si può vedere, la maggior parte del traffico della workstation viene conteggiato nelle statistiche di base TCP o 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
```

Al contrario, una configurazione simile che aggiunge classi specifiche dell'applicazione fornisce statistiche e controlli dell'applicazione più granulari e mantiene la stessa gamma di servizi mostrata nel primo esempio quando si definisce la mappa delle classi dell'ultima occasione che corrisponde solo all'ACL come ultima possibilità nella mappa dei criteri:

```
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
```

La configurazione più specifica fornisce questo output granulare sostanziale per il comando show policy-map type inspect zone-pair priv-pub:

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

   Service-policy inspect : priv-pub-pmap

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

         Session creations since subsystem startup or last reset 731
```

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

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

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

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

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

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

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

```
    Maxever session creation rate 1
    Last half-open session total 0

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

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

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

Un altro vantaggio aggiunto quando si utilizza una configurazione della mappa delle classi e della mappa delle policy più granulare, come accennato in precedenza, è l'opportunità di applicare limiti specifici delle classi ai valori di sessione e velocità; e, in particolare, regolare i parametri di ispezione applicando una mappa di parametri per regolare ogni comportamento di ispezione delle classi.

Configura mapping dei criteri firewall dei criteri basati sulle zone

La mappa dei criteri applica le azioni dei criteri firewall a una o più mappe classi per definire i criteri dei servizi applicati a una coppia di aree di protezione. Quando viene creata una mappa dei criteri di tipo inspect, alla fine della classe viene applicata una classe predefinita denominata class-default. L'azione del criterio predefinita classe-classe è drop ma può essere modificata in pass. L'opzione log può essere aggiunta con l'azione drop. Impossibile applicare Inspect a class-default.

Azioni del firewall dei criteri basati sulle zone

La funzione ZFW effettua tre operazioni per il traffico che attraversa da una zona all'altra:

- Drop: è l'azione predefinita per tutto il traffico, applicata dalla classe class-default che termina ogni mappa dei criteri di tipo inspect. È inoltre possibile configurare altre mappe di classi all'interno di una mappa di criteri per eliminare il traffico indesiderato. Il traffico gestito dall'azione drop viene scartato automaticamente (ossia, non viene inviata alcuna notifica al relativo host finale) dalla ZFW, a differenza del comportamento di un ACL che invia un messaggio ICMP "host unreachable" all'host che ha inviato il traffico negato. Al momento non è disponibile un'opzione per modificare il comportamento della perdita automatica. L'opzione log può essere aggiunta con drop per la notifica syslog che il traffico è stato scartato dal firewall.
- Superato: questa azione consente al router di inoltrare il traffico da una zona all'altra. L'azione

pass non tiene traccia dello stato delle connessioni o delle sessioni all'interno del traffico. Il passaggio consente il traffico in una sola direzione. È necessario applicare una policy parallela per consentire il passaggio del traffico di ritorno nella direzione opposta. L'azione pass è utile per protocolli quali IPSec ESP, IPSec AH, ISAKMP e altri protocolli sicuri che consentono un comportamento prevedibile. Tuttavia, la maggior parte del traffico delle applicazioni viene gestito in modo più efficiente in ZFW con l'azione di ispezione.

- Ispeziona: l'azione ispeziona offre il controllo del traffico basato sullo stato del ciclo di vita. Ad esempio, se viene ispezionato il traffico tra la zona privata e la zona Internet nella precedente rete di esempio, il router conserva le informazioni sulla connessione o sulla sessione per il traffico TCP e UDP (User Datagram Protocol). Pertanto, il router consente il traffico di ritorno inviato dagli host dell'area Internet in risposta alle richieste di connessione all'area privata. Inoltre, inspect può fornire l'ispezione e il controllo delle applicazioni per alcuni protocolli di servizio che possono trasportare traffico di applicazioni vulnerabili o sensibili. L'audit trail può essere applicato con una mappa dei parametri per registrare gli indirizzi di inizio, fine, durata della connessione/sessione, il volume di dati trasferiti e gli indirizzi di origine e di destinazione.

Le azioni sono associate ai mapping delle classi nei mapping dei criteri:

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

Le mappe di parametri offrono opzioni per modificare i parametri di connessione per un determinato criterio di ispezione della mappa di classe.

Configura mapping parametri firewall criteri di zona

Le mappe di parametri specificano il comportamento di ispezione per ZFW, per parametri quali la protezione DoS, i timer di sessione TCP/UDP e l'impostazione della registrazione di riepilogo di controllo. Le mappe dei parametri vengono inoltre applicate con le mappe delle classi e dei criteri del layer 7 per definire il comportamento specifico dell'applicazione, ad esempio oggetti HTTP, requisiti di autenticazione POP3 e IMAP e altre informazioni specifiche dell'applicazione.

Le mappe dei parametri di ispezione per ZFW sono configurate come type inspect, in modo simile ad altri oggetti delle classi e dei criteri 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
```

Tipi specifici di mappe di parametri specificano i parametri applicati dai criteri di ispezione delle applicazioni di layer 7. Le mappe dei parametri di tipo Regex definiscono un'espressione regolare

da utilizzare con l'ispezione dell'applicazione HTTP che filtra il traffico con un'espressione regolare:

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

Le mappe dei parametri di tipo informazioni-protocollo definiscono i nomi dei server da utilizzare con l'ispezione delle applicazioni IM:

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

I dettagli di configurazione completi per l'ispezione delle applicazioni HTTP e IM sono forniti nelle sezioni relative all'ispezione delle applicazioni del presente documento.

Applica registrazione per criteri firewall dei criteri basati su aree

ZFW offre opzioni di registrazione per il traffico che viene scartato o ispezionato per impostazione predefinita o azioni di criteri firewall configurate. La registrazione dell'audit trail è disponibile per il traffico che la ZFW controlla. L'audit trail viene applicato quando un audit trail viene definito in una mappa dei parametri e la mappa dei parametri con l'azione di ispezione viene applicata in una mappa dei criteri:

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

La registrazione della perdita è disponibile per il traffico che viene interrotto dalla ZFW. Il log di eliminazione viene configurato da quando si aggiunge un log con l'azione di eliminazione in una mappa dei criteri:

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

Modifica di mappe classi e mappe criteri del firewall per le zone

Al momento, ZFW non incorpora un editor in grado di modificare le varie strutture ZFW, come le mappe delle policy, le mappe delle classi e le mappe dei parametri. Per ridisporre le istruzioni di corrispondenza in un'applicazione di associazione di classi o di azioni in base alle mappe di classi contenute in una mappa di criteri, è necessario completare i seguenti passaggi:

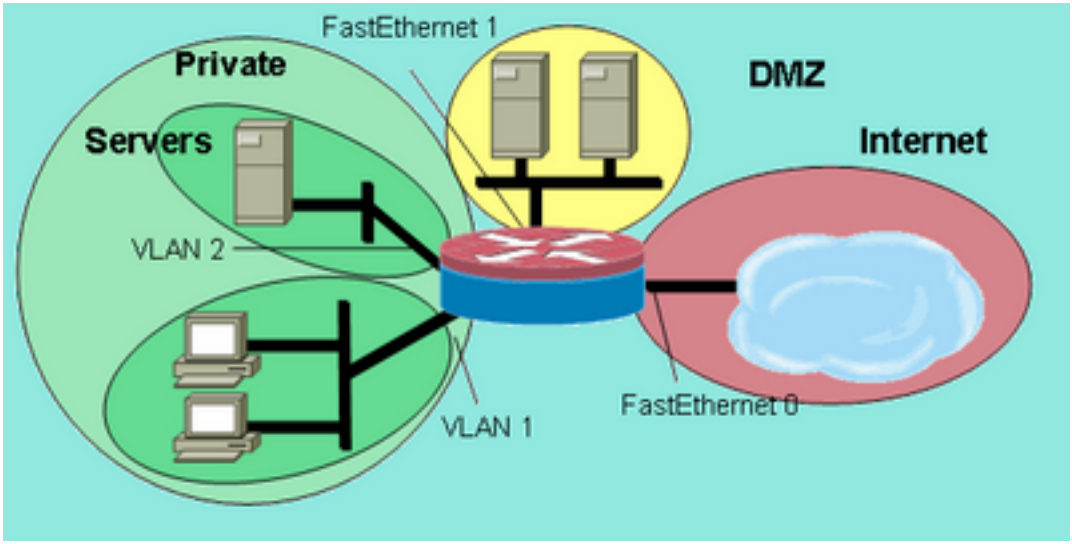
1. Copiare la struttura corrente in un editor di testo quale Blocco note di Microsoft Windows o in un editor quale vi su piattaforme Linux/Unix.
2. Rimuove la struttura corrente dalla configurazione del router.
3. Modificare la struttura nell'editor di testo.
4. Copiare nuovamente la struttura nella CLI del router.

Esempi di configurazione

Questo esempio di configurazione utilizza un Cisco 1811 Integrated Services Router. Una configurazione base con connettività IP, configurazione VLAN e bridging trasparente tra due segmenti LAN Ethernet privati è disponibile nell'Appendice A. Il router è separato in cinque zone:

- Internet pubblica è connessa a FastEthernet 0 (area Internet)
- Due server Internet sono collegati a Fast Ethernet 1 (zona DMZ)
- Lo switch Ethernet è configurato con due VLAN:Le workstation sono collegate alla VLAN1 (zona client).I server sono connessi alla VLAN2 (zona server).Le zone client e server si trovano nella stessa subnet. Tra le zone viene applicato un firewall trasparente, quindi i criteri tra le zone su queste due interfacce possono influire solo sul traffico tra le zone client e server.
- Le interfacce VLAN1 e VLAN2 comunicano con altre reti tramite l'interfaccia virtuale bridge (BVI1). Questa interfaccia è assegnata alla zona privata. (vedere Figura 2).

Figura 2: Dettagli topologia zona

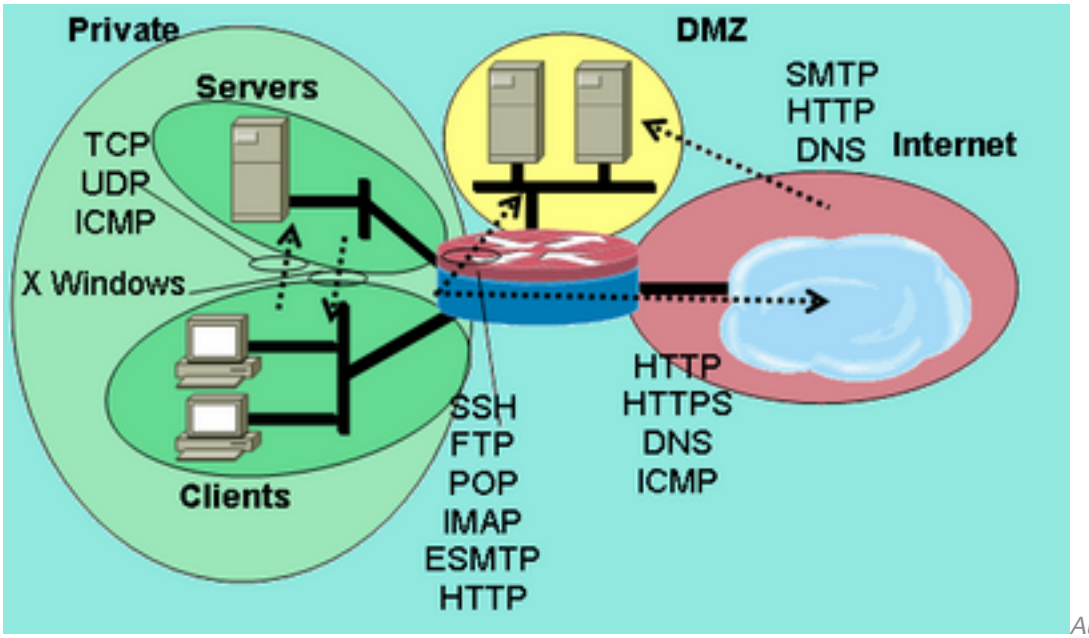


Dettagli topologia zona

Questi criteri vengono applicati con le aree di rete definite in precedenza:

- Gli host nella zona Internet possono raggiungere i servizi DNS, SMTP e SSH su un server nella DMZ. L'altro server offre servizi SMTP, HTTP e HTTPS. I criteri firewall limitano l'accesso ai servizi specifici disponibili in ogni host.
- Gli host DMZ non possono connettersi agli host di altre zone.
- Gli host nella zona client possono connettersi agli host nella zona server su tutti i servizi TCP, UDP e ICMP.
- Gli host nella zona server non possono connettersi agli host nella zona client, ad eccezione di un server applicazioni basato su UNIX che può aprire sessioni client di X Windows a server X Windows su PC desktop nella zona client sulle porte da 6900 a 6910.
- Tutti gli host della zona privata (combinazione di client e server) possono accedere agli host della DMZ sui servizi SSH, FTP, POP, IMAP, ESMTP e HTTP e nella zona Internet sui servizi HTTP, HTTPS, DNS e ICMP. Inoltre, l'ispezione delle applicazioni viene eseguita sulle connessioni HTTP dalla zona privata alla zona Internet in modo da garantire che le applicazioni IM e P2P supportate non vengano trasportate sulla porta 80. (Vedere la Figura 3.)

Figura 3: Autorizzazioni del servizio a coppia di zone da applicare nell'esempio di configurazione



Autorizzazioni del servizio a coppia di zone da applicare nell'esempio di configurazione

Questi criteri firewall sono configurati in ordine di complessità:

1. Ispezione TCP/UDP/ICMP client-server
2. Ispezione Private-DMZ SSH/FTP/POP/IMAP/ESMTP/HTTP
3. Ispezione SMTP/HTTP/DNS Internet -DMZ limitata dall'indirizzo host
4. Ispezione server-client X Windows con un servizio specificato da PAM (Port Application Mapping)
5. Private-Internet HTTP/HTTPS/DNS/ICMP con ispezione dell'applicazione HTTP

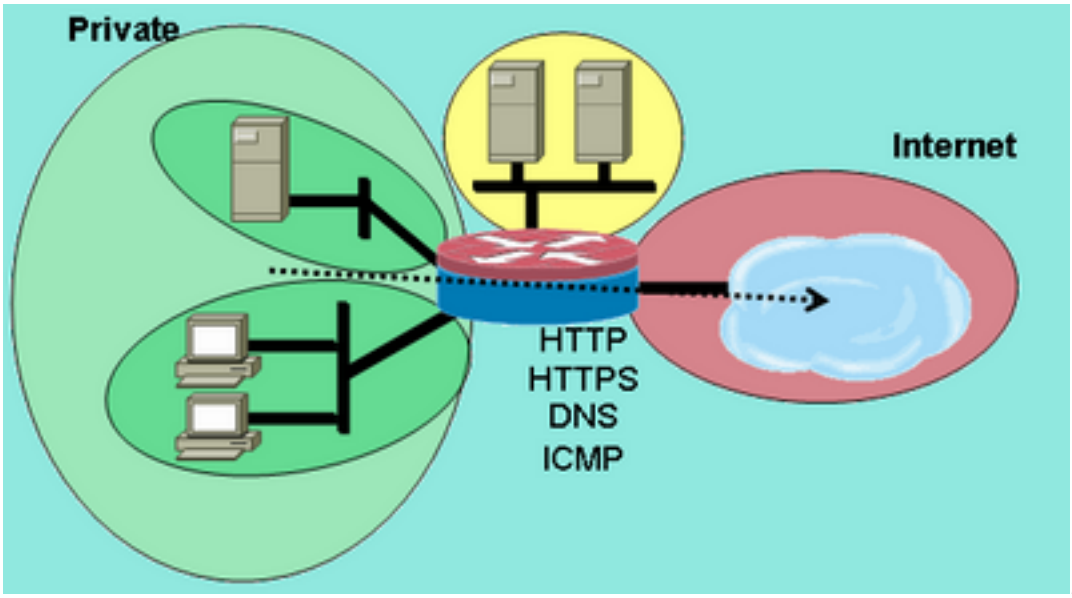
Poiché parti della configurazione vengono applicate a segmenti di rete diversi in momenti diversi, è importante ricordare che un segmento di rete perde la connettività con altri segmenti quando viene posizionato in una zona. Ad esempio, quando viene configurata la zona privata, gli host della zona privata perdono la connettività alle zone DMZ e Internet fino a quando non vengono definiti i rispettivi criteri.

Firewall routing ispezione stateful

Configura criterio Internet privato

La figura 4 illustra la configurazione del criterio Internet privato.

Figura 4: Ispezione dei servizi da zona privata a zona Internet



Ispezione dei servizi da zona privata a zona Internet

Il criterio Internet privato applica l'ispezione di livello 4 all'ispezione di HTTP, HTTPS, DNS e livello 4 per ICMP dalla zona privata alla zona Internet. Questo permette le connessioni dalla zona privata alla zona Internet e permette il traffico di ritorno. L'ispezione di livello 7 offre i vantaggi di un maggiore controllo delle applicazioni, di una maggiore sicurezza e del supporto per le applicazioni che richiedono una correzione. Tuttavia, l'ispezione di layer 7, come accennato, richiede una migliore comprensione dell'attività di rete, in quanto i protocolli di layer 7 non configurati per l'ispezione non sono consentiti tra le zone.

1. Definire mappe di classi che descrivono il traffico che si desidera autorizzare tra le zone, in base ai criteri descritti in precedenza:
```
configure terminal
 class-map type inspect match-any internet-traffic-class
  match protocol http
  match protocol https
  match protocol dns
  match protocol icmp
```
2. Configurare una mappa criteri per ispezionare il traffico sulle mappe classi appena definite:
```
configure terminal
 policy-map type inspect private-internet-policy
  class type inspect internet-traffic-class
   inspect
```
3. Configurare le zone private e Internet e assegnare le interfacce router alle rispettive zone:
```
configure terminal
 zone security private
 zone security internet
 int bvi1
  zone-member security private
 int fastethernet 0
  zone-member security internet
```

Configurare la coppia di zone e applicare la mappa dei criteri appropriata.

> **Nota:** È sufficiente configurare la coppia di aree Internet private per controllare le connessioni originate nella zona privata che viaggiano verso l'area Internet, come mostrato di seguito:

```
configure terminal
 zone-pair security private-internet source private destination internet
```

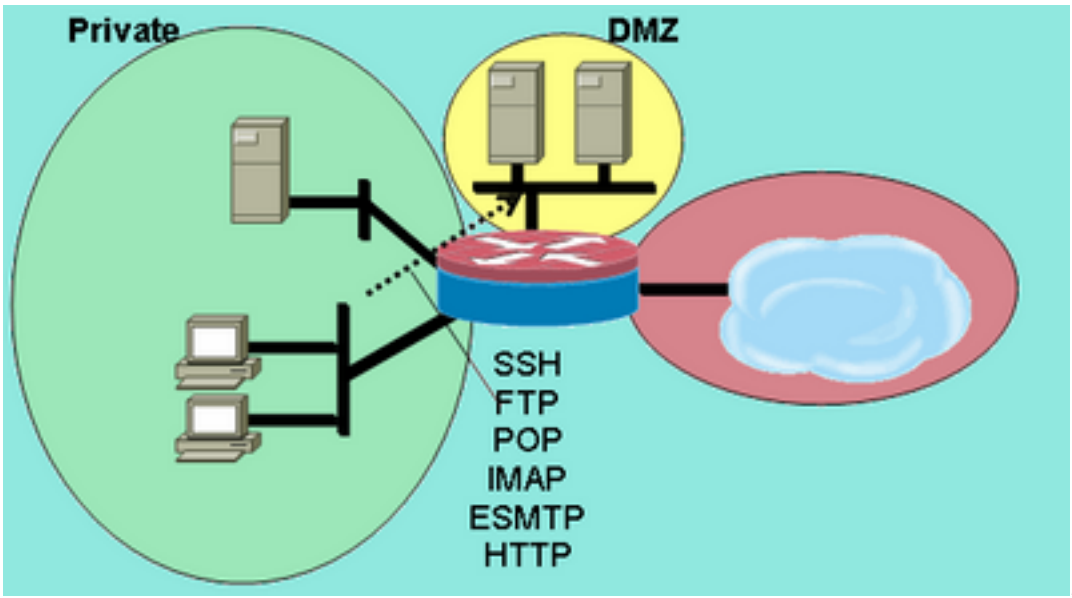
```
service-policy type inspect private-internet-policy
```

La configurazione del criterio di ispezione di layer 7 sulla coppia di zone Internet private è completata per consentire connessioni HTTP, HTTPS, DNS e ICMP dalla zona client alla zona server e per applicare l'ispezione delle applicazioni al traffico HTTP in modo da assicurare che il traffico indesiderato non possa passare su TCP 80, la porta del servizio HTTP.

Configura criterio DMZ privato

Nella figura 5 viene illustrata la configurazione della policy DMZ privata.

Figura 5: Ispezione dei servizi da zona privata a zona DMZ



Ispezione dei servizi da zona privata a zona DMZ

I criteri privati DMZ aggiungono complessità poiché richiedono una migliore comprensione del traffico di rete tra le zone. Questo criterio applica l'ispezione di layer 7 dalla zona privata alla zona dinamica dei dischi. Questo permette le connessioni dalla zona privata alla zona demilitarizzata e permette il traffico di ritorno. L'ispezione di livello 7 offre i vantaggi di un maggiore controllo delle applicazioni, di una maggiore sicurezza e del supporto per le applicazioni che richiedono una correzione. Tuttavia, l'ispezione di layer 7, come accennato, richiede una migliore comprensione dell'attività di rete, in quanto i protocolli di layer 7 non configurati per l'ispezione non sono consentiti tra le zone.

1. Definire mappe di classi che descrivono il traffico che si desidera autorizzare tra le zone, in base ai criteri descritti in precedenza:
```
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. Configurare i mapping delle policy per ispezionare il traffico sui mapping delle classi appena definiti:
```
configure terminal
 policy-map type inspect private-dmz-policy
  class type inspect L7-inspect-class
   inspect
```

3. Configurare le zone private e DMZ e assegnare le interfacce router alle rispettive zone:

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

4. Configurare la coppia di zone e applicare la mappa dei criteri appropriata.

   Nota: Al momento è sufficiente configurare la coppia di zone DMZ private per ispezionare le connessioni originate nella zona privata che viaggiano verso la zona DMZ, come mostrato di seguito:

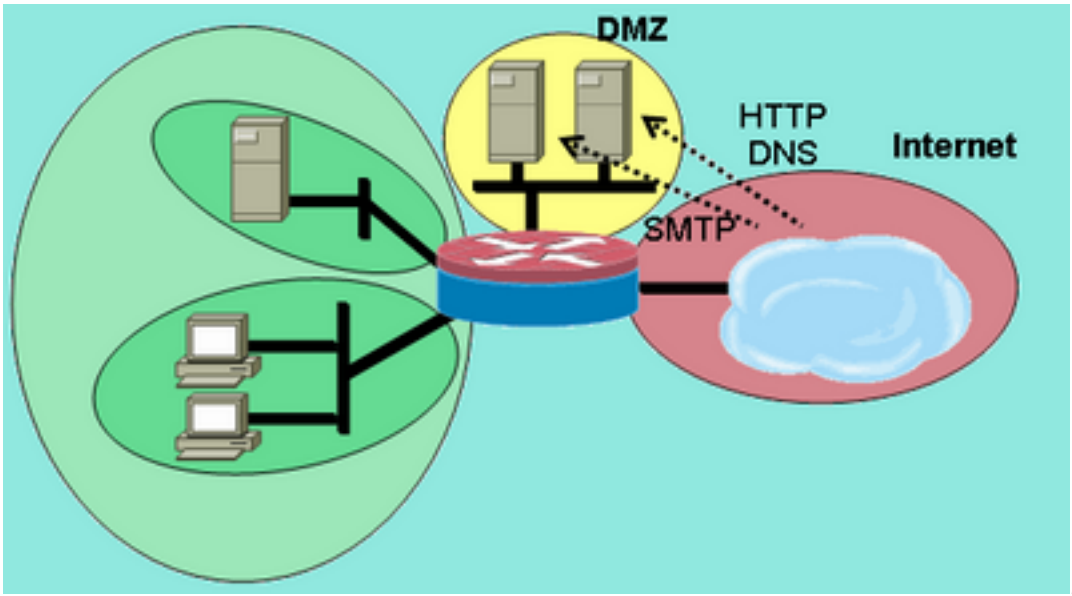
```
configure terminal
 zone-pair security private-dmz source private destination dmz
  service-policy type inspect private-dmz-policy
```

La configurazione del criterio di ispezione di layer 7 sulla DMZ privata è stata completata per consentire tutte le connessioni TCP, UDP e ICMP dalla zona client alla zona server. Il criterio non applica la correzione per i canali subordinati, ma fornisce un esempio di criterio semplice per la maggior parte delle connessioni delle applicazioni.

Configura criterio DMZ Internet

La figura 6 illustra la configurazione della policy DMZ Internet.

Figura 6: Ispezione dei servizi dall'area Internet alla zona DMZ



Ispezione dei servizi dall'area Internet alla zona DMZ

Questo criterio applica l'ispezione di livello 7 dall'area Internet alla DMZ. Questo consente le connessioni dalla zona Internet alla zona demilitarizzata e permette il traffico di ritorno dagli host della zona demilitarizzata agli host Internet da cui è stata originata la connessione. Il criterio DMZ Internet combina l'ispezione di layer 7 con i gruppi di indirizzi definiti dagli ACL per limitare l'accesso a servizi specifici su host, gruppi di host o subnet specifici. A tale scopo, nidificare una mappa delle classi che specifica i servizi all'interno di un'altra mappa delle classi che fa riferimento a un ACL per specificare gli indirizzi IP.

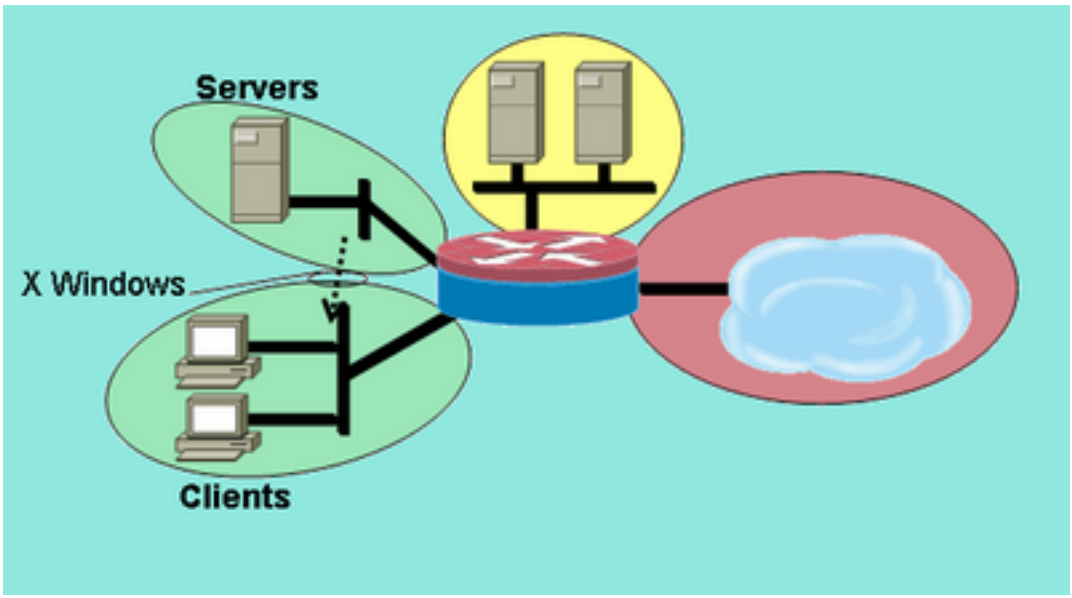
1. Definire class-map e ACL che descrivono il traffico che si desidera autorizzare tra le zone, in base ai criteri descritti in precedenza.Ènecessario utilizzare più mappe di classe per i servizi, poiché vengono applicati criteri di accesso diversi per l'accesso a due server diversi. Gli host Internet possono utilizzare connessioni DNS e HTTP a 172.16.2.2, mentre le connessioni SMTP a 172.16.2.3. Si noti la differenza nelle mappe di classe. Le mappe di classe che specificano i servizi utilizzano la parola chiave match-any per consentire uno dei servizi elencati. Le mappe di classe che associano gli ACL alle mappe di classe del servizio utilizzano la parola chiave match-all per richiedere che entrambe le condizioni nella mappa di classe siano soddisfatte per consentire il traffico:
```
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. Configurare i mapping delle policy per ispezionare il traffico sui mapping delle classi appena definiti:
```
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. Configurare le zone Internet e DMZ e assegnare le interfacce router alle rispettive zone. Ignorare la configurazione DMZ se la si è impostata nella sezione precedente:
```
configure terminal
zone security internet
zone security dmz
int fastethernet 0
 zone-member security internet
int fastethernet 1
 zone-member security dmz
```
4. Configurare la coppia di zone e applicare la mappa dei criteri appropriata.**Nota:** Al momento è sufficiente configurare la coppia di zone DMZ Internet per ispezionare le connessioni originate nell'area Internet che viaggiano verso la zona DMZ, come mostrato di seguito:
```
configure terminal
 zone-pair security internet-dmz source internet destination dmz
  service-policy type inspect internet-dmz-policy
```
La configurazione del criterio di ispezione Layer 7 specifico dell'indirizzo sulla coppia di zone DMZ Internet è stata completata.

Firewall trasparente ispezione stateful

Configura criterio server-client

Nella figura seguente viene illustrata la configurazione dei criteri server-client.

Figura 7: Ispezione dei servizi dall'area Server all'area Client



Ispezione dei servizi dall'area Server all'area Client

Il criterio server-client applica l'ispezione con un servizio definito dall'utente. L'ispezione di livello 7 viene applicata dalla zona server alla zona client. Ciò consente le connessioni X Windows a un intervallo di porte specifico dalla zona server alla zona client e permette il traffico di ritorno. X Windows non è un protocollo nativo supportato in PAM, quindi è necessario definire un servizio configurato dall'utente in PAM in modo che ZFW possa riconoscere e ispezionare il traffico appropriato.

Due o più interfacce router sono configurate in un bridge-group IEEE per fornire il routing e il bridging integrati (IRB) per fornire il bridging tra le interfacce nel bridge-group e per indirizzare ad altre subnet tramite BVI (Bridge Virtual Interface). La policy del firewall trasparente applica l'ispezione del firewall per il traffico che "attraversa il ponte", ma non per il traffico che lascia il gruppo di bridge attraverso il BVI. La politica in materia di ispezioni si applica solo al traffico che attraversa il gruppo-ponte. Pertanto, in questo scenario, l'ispezione viene applicata solo al traffico che si sposta tra le zone client e server, nidificate all'interno della zona privata. La policy applicata tra la zona privata, e le zone pubbliche e DMZ, entra in gioco solo quando il traffico lascia il gruppo-ponte attraverso il BVI. Quando il traffico parte attraverso il BVI dalle zone client o server, non viene richiamata la policy del firewall trasparente.

1. Configurare PAM con una voce definita dall'utente per X Windows.I client X Windows (in cui sono ospitate le applicazioni) aprono le connessioni per visualizzare le informazioni sui client (in cui l'utente lavora) in un intervallo che inizia dalla porta 6900.Ogni connessione aggiuntiva utilizza porte successive, quindi se un client visualizza 10 sessioni diverse su un host, il server utilizza le porte 6900-6909. Pertanto, se si controlla l'intervallo di porte da 6900 a 6909, le connessioni aperte su porte oltre 6909 hanno esito negativo:
```
configure terminal
 ip port-map user-Xwindows port tcp from 6900 to 6910
```
2. Esaminare i documenti PAM per risolvere altre domande su PAM o controllare la documentazione relativa all'ispezione del protocollo granulare per informazioni sui dettagli dell'interoperabilità tra PAM e Cisco IOS Firewall con controllo dello stato.
3. Definire mappe di classi che descrivono il traffico che si desidera autorizzare tra le zone, in base ai criteri descritti in precedenza:
```
configure terminal
 class-map type inspect match-any Xwindows-class
```

```
  match protocol user-Xwindows
```

4. Configurare i mapping delle policy per ispezionare il traffico sui mapping delle classi appena definiti:

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

5. Configurare le zone client e server e assegnare le interfacce router alle rispettive zone.Se queste zone sono state configurate e le interfacce assegnate nella sezione Configurazione criteri client-server, è possibile passare alla definizione della coppia di zone. La configurazione IRB di bridging viene fornita per completezza:

```
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. Configurare la coppia di zone e applicare la mappa dei criteri appropriata.**Nota:** È sufficiente configurare la coppia di zone server-client per controllare le connessioni originate nella zona server che viaggiano verso la zona client, come mostrato di seguito:

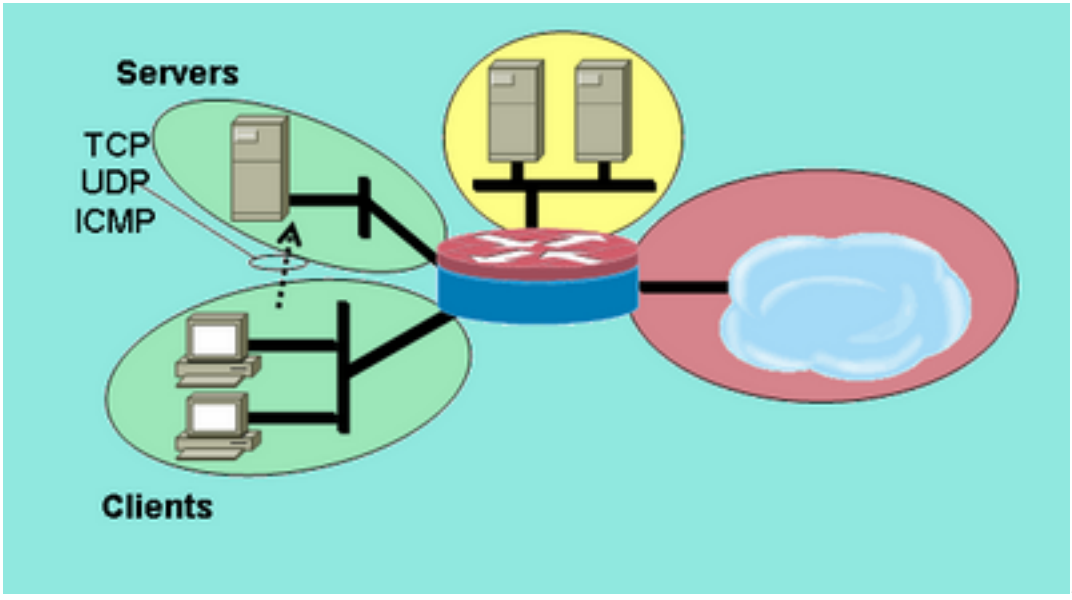
```
configure terminal
 zone-pair security servers-clients source servers destination clients
  service-policy type inspect servers-clients-policy
```

   La configurazione del criterio di ispezione definito dall'utente nella coppia di zone server-client è stata completata per consentire le connessioni X Windows dalla zona server alla zona client.

Configura criterio client-server

La figura 8 illustra la configurazione della policy client-server.

Figura 8: Ispezione dei servizi dalla zona client alla zona server



Ispezione dei servizi dalla

zona client alla zona server

Il criterio client-server è meno complesso degli altri. L'ispezione di livello 4 viene applicata dalla zona client alla zona server. Questo consente le connessioni dalla zona client alla zona server e permette il traffico di ritorno. L'ispezione di layer 4 offre il vantaggio della semplicità nella configurazione del firewall, in quanto sono necessarie solo poche regole per consentire la maggior parte del traffico delle applicazioni. Tuttavia, l'ispezione del layer 4 comporta anche due svantaggi principali:

- Le applicazioni quali i servizi FTP o multimediali spesso negoziano un canale subordinato aggiuntivo dal server al client. Questa funzionalità viene generalmente implementata in una correzione del servizio che controlla la finestra di dialogo del canale di controllo e consente al canale subordinato. Questa funzionalità non è disponibile nell'ispezione di layer 4.
- L'ispezione di livello 4 consente di gestire quasi tutto il traffico a livello di applicazione. Se è necessario controllare l'utilizzo della rete in modo da consentire solo poche applicazioni attraverso il firewall, è necessario configurare un ACL sul traffico in uscita per limitare i servizi consentiti attraverso il firewall.

Entrambe le interfacce router sono configurate in un gruppo di bridge IEEE, pertanto questo criterio firewall applica un'ispezione trasparente del firewall. Questo criterio viene applicato a due interfacce in un gruppo di bridge IP IEEE. I criteri di ispezione si applicano solo al traffico che attraversa il gruppo di bridge. Questo spiega perché le zone client e server sono nidificate all'interno della zona privata.

1. Definire mappe di classi che descrivono il traffico che si desidera autorizzare tra le zone, in base ai criteri descritti in precedenza:
```
configure terminal
 class-map type inspect match-any L4-inspect-class
 match protocol tcp
 match protocol udp
 match protocol icmp
```
2. Configurare i mapping delle policy per ispezionare il traffico sui mapping delle classi appena definiti:
```
configure terminal
 policy-map type inspect clients-servers-policy
 class type inspect L4-inspect-class
  inspect
```
3. Configurare le zone client e server e assegnare le interfacce router alle rispettive zone:
```
configure terminal
 zone security clients
 zone security servers
 interface vlan 1
  zone-member security clients
 interface vlan 2
  zone-member security servers
```
4. Configurare la coppia di zone e applicare la mappa dei criteri appropriata.**Nota:** È sufficiente configurare la coppia di zone client-server per controllare le connessioni originate nella zona client che viaggiano verso la zona server, come mostrato di seguito:
```
configure terminal
 zone-pair security clients-servers source clients destination servers
  service-policy type inspect clients-servers-policy
```
La configurazione del criterio di ispezione di layer 4 per la coppia di zone client-server è stata completata per consentire tutte le connessioni TCP, UDP e ICMP dalla zona client alla zona server. Il criterio non applica la correzione per i canali subordinati, ma fornisce un esempio di criterio semplice per la maggior parte delle connessioni delle applicazioni.

Criteri di velocità per il firewall dei criteri basato su zone

Le reti di dati spesso traggono vantaggio dalla capacità di limitare la velocità di trasmissione di tipi specifici di traffico di rete e di limitare l'impatto del traffico con priorità inferiore a un traffico più essenziale per l'azienda. Il software Cisco IOS offre questa funzionalità con il traffic policing , che limita la velocità nominale del traffico e i burst. Il software Cisco IOS supporta il monitoraggio del traffico da Cisco IOS versione 12.1(5)T.

Il software Cisco IOS versione 12.4(9)T aumenta la velocità ZFW quando si aggiunge al traffico di polizia una funzionalità che corrisponde alle definizioni di una class-map specifica mentre attraversa il firewall da un'area di sicurezza all'altra. Ciò offre la praticità di un punto di configurazione per descrivere il traffico specifico, applicare i criteri firewall e controllare l'utilizzo della larghezza di banda del traffico. ZFW si differenzia da interface-based in quanto fornisce solo le azioni di trasmissione per la conformità ai criteri e di rilascio per la violazione dei criteri. ZFW non può contrassegnare il traffico per DSCP.

ZFW può specificare l'uso della larghezza di banda solo in byte al secondo, pacchetto al secondo e percentuale di larghezza di banda non sono offerti. ZFW può essere applicato con o senza interfaccia. Pertanto, se sono necessarie funzionalità aggiuntive, queste possono essere applicate in base all'interfaccia. Se l'interfaccia basata su viene utilizzata insieme al firewall, verificare che i criteri non siano in conflitto.

Configura criterio ZFW

Il policing ZFW limita il traffico in una mappa delle classi basata su policy a un valore di velocità definito dall'utente compreso tra 8.000 e 2.000.000.000 di bit al secondo, con un valore burst configurabile compreso tra 1.000 e 512.000.000 di byte.

Il policing ZFW è configurato da una linea di configurazione aggiuntiva nella mappa dei criteri, che viene applicata dopo l'azione:

```
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>]
```

Controllo della sessione

Il criterio ZFW ha inoltre introdotto il controllo delle sessioni per limitare il conteggio delle sessioni per il traffico in una mappa dei criteri che corrisponde a una mappa delle classi. In questo modo si aggiunge la funzionalità corrente di applicazione dei criteri di protezione DoS per mappa di classe. Ciò consente un controllo granulare del numero di sessioni che corrispondono a una determinata mappa di classe che attraversa una coppia di zone. Se la stessa mappa di classe viene utilizzata in più mappe di criteri o coppie di zone, è possibile applicare limiti di sessione diversi alle varie applicazioni di mappa di classe.

Il controllo della sessione viene applicato quando viene configurata una mappa dei parametri contenente il volume di sessione desiderato, quindi la mappa dei parametri viene aggiunta all'azione di ispezione applicata a una mappa delle classi in una mappa dei criteri:

```
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
```

Le mappe di parametri possono essere applicate solo all'azione di ispezione e non sono disponibili nelle azioni di tipo pass o drop.

Le attività di controllo e applicazione di policy della sessione ZFW sono visibili con questo comando:

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

Ispezione applicazione

L'ispezione delle applicazioni introduce funzionalità aggiuntive per ZFW. I criteri di ispezione delle applicazioni vengono applicati al livello 7 del modello OSI, in cui le applicazioni utente inviano e ricevono messaggi che consentono alle applicazioni di offrire funzionalità utili. Alcune applicazioni possono offrire funzionalità indesiderate o vulnerabili, pertanto i messaggi associati a tali funzionalità devono essere filtrati per limitare le attività sui servizi delle applicazioni.

Cisco IOS Software ZFW offre l'ispezione e il controllo delle applicazioni su questi servizi:

- HTTP
- SMTP
- POP3
- IMAP
- Sun RPC
- Traffico applicazioni P2P
- Applicazioni IM

La capacità di ispezione e controllo delle applicazioni (AIC) varia in base al servizio. L'ispezione HTTP offre un filtro granulare su diversi tipi di attività delle applicazioni e fornisce funzionalità per limitare le dimensioni del trasferimento, la lunghezza degli indirizzi Web e l'attività del browser, al fine di garantire la conformità agli standard di comportamento delle applicazioni e limitare i tipi di contenuto trasferiti tramite il servizio. AIC per SMTP può limitare la lunghezza del contenuto e applicare la conformità del protocollo. L'ispezione POP3 e IMAP consente di garantire che gli utenti utilizzino meccanismi di autenticazione sicuri per evitare la compromissione delle credenziali utente.

L'ispezione delle applicazioni viene configurata come un set aggiuntivo di mappe delle classi e mappe dei criteri specifiche dell'applicazione, che vengono quindi applicate alle mappe delle classi e alle mappe dei criteri di ispezione correnti in base a quando si definisce il criterio del servizio dell'applicazione nella mappa dei criteri di ispezione.

Ispezione applicazione HTTP

L'ispezione delle applicazioni può essere applicata al traffico HTTP per controllare l'utilizzo indesiderato della porta del servizio HTTP per altre applicazioni quali IM, condivisione file P2P e applicazioni di tunneling in grado di reindirizzare le applicazioni firewall tramite TCP 80.

Configurare una mappa delle classi di ispezione delle applicazioni per descrivere il traffico che

viola il traffico HTTP consentito:

```
! 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
```

Miglioramenti HTTP Application Inspection

Il software Cisco IOS versione 12.4(9)T introduce miglioramenti alle funzionalità di ispezione HTTP di ZFW. Cisco IOS Firewall ha introdotto la funzionalità HTTP Application Inspection nel software Cisco IOS versione 12.3(14)T. Il software Cisco IOS versione 12.4(9)T aumenta le funzionalità correnti quando si aggiungono:

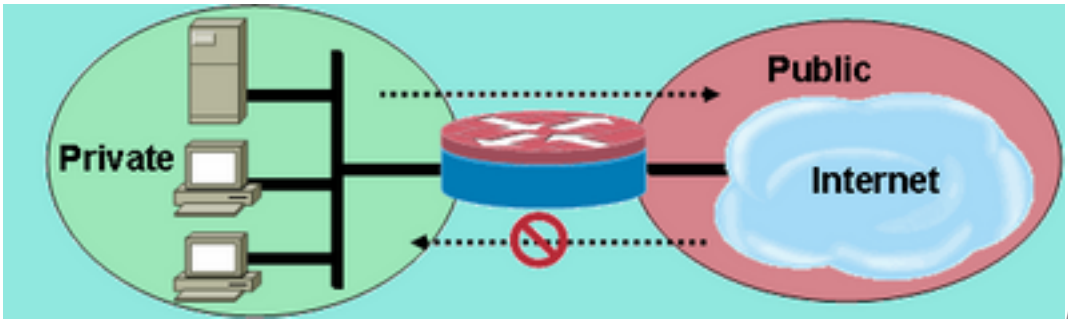
- Possibilità di autorizzare, negare e monitorare le richieste e le risposte in base al nome dell'intestazione e ai valori dell'intestazione. Questa opzione è utile per bloccare le richieste e le risposte che contengono campi di intestazione vulnerabili.
- Possibilità di limitare le dimensioni dei diversi elementi nelle intestazioni delle richieste e delle risposte HTTP, ad esempio la lunghezza massima dell'URL, la lunghezza massima dell'intestazione, il numero massimo di intestazioni, la lunghezza massima della riga di intestazione e così via. Ciò è utile per evitare l'overflow del buffer.
- Possibilità di bloccare richieste e risposte che contengono più intestazioni dello stesso tipo. ad esempio, una richiesta con due intestazioni content-length.
- Possibilità di bloccare richieste e risposte con intestazioni non ASCII. Ciò è utile per prevenire vari attacchi che utilizzano caratteri binari e altri caratteri non ASCII per distribuire worm e altri contenuti dannosi ai server Web.
- Possibilità di raggruppare i metodi HTTP in categorie specificate dall'utente e flessibilità per bloccare/consentire/monitorare ciascun gruppo. L'RFC HTTP consente un set limitato di metodi HTTP. Alcuni metodi standard sono considerati non sicuri perché possono essere utilizzati per sfruttare le vulnerabilità su un server Web. Molti metodi non standard hanno un record di protezione non valido.
- Metodo per bloccare URI specifici in base a un'espressione regolare configurata dall'utente. Questa funzionalità consente all'utente di bloccare le query e gli URI personalizzati.
- Possibilità di contraffare i tipi di intestazione (in particolare il tipo di intestazione del server)

con stringhe personalizzabili dall'utente. Ciò è utile nel caso in cui un utente malintenzionato analizza le risposte del server Web e apprende quante più informazioni possibili, quindi lancia un attacco che sfrutta le debolezze di quel particolare server Web.

- Possibilità di bloccare o inviare un avviso su una connessione HTTP se uno o più valori dei parametri HTTP corrispondono ai valori immessi dall'utente come espressione regolare. Alcuni dei possibili contesti dei valori HTTP includono intestazione, corpo, nome utente, password, agente utente, riga di richiesta, riga di stato e variabili CGI decodificate.

Gli esempi di configurazione per i miglioramenti del controllo delle applicazioni HTTP presuppongono una rete semplice, come illustrato nella Figura 9.

Figura 9: Ispezione delle applicazioni Presupponi una rete semplice



Ispezione delle applicazioni Presupponi una rete semplice

Il firewall raggruppa il traffico in due classi:

- traffico HTTP
- Tutto il resto del traffico TCP, UDP e ICMP a canale singolo

Il protocollo HTTP è separato per consentire l'ispezione specifica sul traffico Web. In questo modo è possibile configurare il controllo dei criteri nella prima sezione di questo documento e il controllo delle applicazioni HTTP nella seconda sezione. Nella terza sezione di questo documento è possibile configurare mappe delle classi e mappe dei criteri specifiche per il traffico P2P e IM. La connettività dalla zona privata alla zona pubblica è consentita. Nessuna connettività dalla zona pubblica alla zona privata.

Fare riferimento all'Appendice C per una configurazione completa che implementa la policy iniziale.

Configura miglioramenti controllo applicazione HTTP

Il controllo delle applicazioni HTTP (nonché altri criteri di controllo delle applicazioni) richiede una configurazione più complessa rispetto alla configurazione di base del layer 4. È necessario configurare la classificazione del traffico di layer 7 e i criteri in modo da riconoscere il traffico specifico che si desidera controllare e applicare l'azione desiderata al traffico desiderato e non desiderato.

L'ispezione delle applicazioni HTTP (simile ad altri tipi di ispezione delle applicazioni) può essere applicata solo al traffico HTTP. È quindi necessario definire mappe di classe e mappe di policy di layer 7 per il traffico HTTP specifico, quindi definire una mappa di classe di layer 4 specificamente per HTTP e applicare il criterio di layer 7 all'ispezione HTTP in una mappa di policy di layer 4, come indicato di seguito:

```
!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
```

Tutte queste caratteristiche del traffico HTTP Application Inspection sono definite in una mappa di classe di layer 7:

- Il comando Ispezione intestazione consente di autorizzare/negare/monitorare le richieste o le risposte la cui intestazione corrisponde all'espressione regolare configurata. È possibile applicare l'azione Consenti o Reimposta a una richiesta o risposta che corrisponde ai criteri della mappa di classe. L'aggiunta dell'azione log causa un messaggio syslog: `APPFW-6-HTTP_HDR_REGEX_MATCHED`
  Utilizzo comando:

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

Esempio di caso di utilizzo

- Configurare un criterio http appfw per bloccare la richiesta o la risposta la cui intestazione contiene caratteri 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
```

Ispezione lunghezza intestazione - Questo comando controlla la lunghezza di un'intestazione di richiesta o di risposta e applica l'azione se la lunghezza supera la soglia configurata. Azione consentita o reimpostata. L'aggiunta dell'azione log causa un messaggio syslog:

```
APPFW-4- HTTP_HEADER_LENGTH
```

Utilizzo comando:

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

Esempio di caso di utilizzo

Configurare un criterio http appfw per bloccare le richieste e le risposte con una lunghezza di intestazione superiore a 4096 byte.

```
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
```

Ispezione conteggio intestazioni - Questo comando verifica il numero di righe di intestazione (campi) in una richiesta/risposta e applica un'azione quando il conteggio supera la soglia configurata. Azione consentita o reimpostata. L'aggiunta dell'azione log causa un messaggio syslog:

```
APPFW-6- HTTP_HEADER_COUNT
```

Utilizzo comando:

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

Esempio di caso di utilizzo

Configurare un criterio http appfw per bloccare una richiesta con più di 16 campi di intestazione.

```
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
```

Ispezione campo intestazione - Questo comando consente di autorizzare/negare/monitorare le richieste/risposte che contengono un valore e un campo intestazione HTTP specifici. È possibile applicare l'azione Consenti o Reimposta a una richiesta o risposta che corrisponde ai criteri della mappa di classe. L'aggiunta dell'azione log causa un messaggio syslog:

```
APPFW-6- HTTP_HDR_FIELD_REGEX_MATCHED
```

Utilizzo comando:

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

Esempio di caso di utilizzo

Configurare un criterio di ispezione dell'applicazione HTTP per bloccare 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
```

Ispezione lunghezza campo intestazione - Questo comando consente di limitare la lunghezza di una riga del campo intestazione. È possibile applicare l'azione Consenti o Reimposta a una richiesta o risposta che corrisponde ai criteri della mappa di classe. L'aggiunta dell'azione log causa un messaggio syslog:

```
APPFW-6- HTTP_HDR_FIELD_LENGTH
```

Utilizzo comando:

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

Esempio di caso di utilizzo

Configurare un criterio http appfw per bloccare una richiesta il cui cookie e la lunghezza del campo agente utente superano rispettivamente 256 e 128.

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

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

Ispezione della ripetizione del campo dell'intestazione - Questo comando controlla se una richiesta o una risposta contiene campi di intestazione ripetuti. È possibile applicare l'azione Consenti o Reimposta a una richiesta o risposta che corrisponde ai criteri della mappa di classe. Quando è abilitata, l'azione log genera un messaggio syslog:

```
APPFW-6- HTTP_REPEATED_HDR_FIELDS
```

Utilizzo comando:

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

Esempio di caso di utilizzo

Configurare un criterio http appfw per bloccare una richiesta o una risposta con più righe di intestazione di lunghezza contenuto. Questa è una delle funzionalità più utili per prevenire il contrabbando delle sessioni.

```
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
```

- Ispezione di metodo: l'RFC HTTP consente un set limitato di metodi HTTP. Tuttavia, anche alcuni dei metodi standard sono considerati non sicuri in quanto alcuni metodi possono essere utilizzati per sfruttare le vulnerabilità su un server Web. Molti dei metodi non standard vengono utilizzati frequentemente per attività dannose. È quindi necessario raggruppare i metodi in varie categorie e fare in modo che l'utente scelga l'azione per ciascuna categoria. Questo comando fornisce all'utente un modo flessibile per raggruppare i metodi in varie categorie, ad esempio metodi sicuri, metodi non sicuri, metodi webdav, metodi RFC e metodi estesi. È possibile applicare l'azione Consenti o Reimposta a una richiesta o risposta che corrisponde ai criteri della mappa di classe. L'aggiunta dell'azione log causa un messaggio syslog:

```
APPFW-6-HTTP_METHOD
```

Utilizzo comando:

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

Esempio di caso di utilizzo

Configurare un criterio http appfw che raggruppa i metodi HTTP in tre categorie: safe, unsafe e webdav. Questi sono illustrati nella tabella seguente. Configurare le azioni in modo che:

- Tutti i metodi sicuri sono consentiti senza registro
- Tutti i metodi unsafe sono consentiti con il registro
- Tutti i metodi webdav sono bloccati dal log.

Sicuro	Non sicuro	WebDAV
GET, HEAD, OPTION	POST, PUT, CONNECT, TRACE	BCOPY, BDELETE E 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
```

Ispezione URI: questo comando consente di autorizzare/negare/monitorare le richieste il cui URI corrisponde all'ispezione regolare configurata. In questo modo, è possibile bloccare URL e query personalizzati. È possibile applicare l'azione Consenti o Reimposta a una richiesta o risposta che corrisponde ai criteri della mappa di classe. L'aggiunta dell'azione log causa un messaggio syslog:

```
APPFW-6- HTTP_URI_REGEX_MATCHED
```

Utilizzo comando:

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

Esempio di caso di utilizzo

Configurare un criterio http appfw per bloccare una richiesta il cui URI corrisponde a una delle seguenti espressioni regolari:

- .*cmd.exe
- .*sesso
- .*gioco d'azzardo

```
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
```

- Ispezione lunghezza URI — Questo comando verifica la lunghezza dell'URI inviato in una richiesta e applica l'azione configurata quando la lunghezza supera la soglia configurata. È possibile applicare l'azione Consenti o Reimposta a una richiesta o risposta che corrisponde ai criteri della mappa di classe. L'aggiunta dell'azione log causa un messaggio syslog:
  ```
  APPFW-6- HTTP_URI_LENGTH
  ```
  Utilizzo comando:
  ```
  match request uri length gt <bytes>
  ```
  Esempio di caso di utilizzo

Configurare un criterio http appfw per generare un avviso ogni volta che la lunghezza URI di una richiesta supera i 3076 byte.

```
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
```

Ispezione argomenti - Questo comando consente di autorizzare, negare o monitorare le richieste i cui argomenti (parametri) corrispondono all'ispezione regolare configurata. È possibile applicare l'azione Consenti o Reimposta a una richiesta o risposta che corrisponde ai criteri della mappa di classe. L'aggiunta dell'azione log causa un messaggio syslog:

APPFW-6- HTTP_ARG_REGEX_MATCHED

Utilizzo comando:

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

Configurare un criterio http appfw per bloccare una richiesta i cui argomenti corrispondono a una delle seguenti espressioni regolari:

- .*codificato
- .*attacco

```
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
```

- Ispezione della lunghezza degli argomenti: questo comando verifica la lunghezza degli argomenti inviati in una richiesta e applica l'azione configurata quando la lunghezza supera la soglia configurata. È possibile applicare l'azione Consenti o Reimposta a una richiesta o risposta che corrisponde ai criteri della mappa di classe. L'aggiunta dell'azione log causa un messaggio syslog:

  APPFW-6- HTTP_ARG_LENGTH

  Utilizzo comando:

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

  Esempio di caso di utilizzo

Configurare un criterio http appfw per generare un avviso ogni volta che la lunghezza degli argomenti di una richiesta supera i 512 byte.

```
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
```

- Controllo del corpo - Questa CLI consente all'utente di specificare una lista di espressioni regolari da confrontare con il corpo della richiesta o della risposta. È possibile applicare l'azione Consenti o Reimposta a una richiesta o risposta che corrisponde ai criteri della mappa di classe. L'aggiunta dell'azione log causa un messaggio syslog:

  APPFW-6- HTTP_BODY_REGEX_MATCHED

  Utilizzo comando:

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

  Esempio di caso di utilizzo

Configurare un'app http per bloccare una risposta il cui corpo contiene il modello `.*[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
```

Ispezione lunghezza corpo (contenuto) - Questo comando verifica le dimensioni del messaggio inviato tramite richiesta o risposta. È possibile applicare l'azione Consenti o Reimposta a una richiesta o risposta che corrisponde ai criteri della mappa di classe. L'aggiunta dell'azione log causa un messaggio syslog:

```
APPFW-4- HTTP_CONTENT_LENGTH
```

Utilizzo comando:

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

Esempio di caso di utilizzo

Configurare un criterio http appfw per bloccare una sessione http che trasporta più di 10K byte di messaggio in una richiesta o risposta.

```
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
```

Ispezione della riga di stato - Il comando consente all'utente di specificare un elenco di espressioni regolari da confrontare con la riga di stato di una risposta. È possibile applicare l'azione Consenti o Reimposta a una richiesta o risposta che corrisponde ai criteri della mappa di classe. L'aggiunta dell'azione log causa un messaggio syslog:

```
APPFW-6-HTTP_STLINE_REGEX_MATCHED
```

Utilizzo comando:

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

Esempio di caso di utilizzo

Configurare un http appfw per registrare un avviso ogni volta che si tenta di accedere a una pagina vietata. Una pagina vietata contiene in genere un codice di stato 403 e la riga di stato è simile a `HTTP/1.0 403 pagina vietata\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
```

- Controllo tipo di contenuto - Questo comando verifica se il tipo di contenuto dell'intestazione del messaggio è presente nell'elenco dei tipi di contenuto supportati. Verifica inoltre che il tipo di contenuto dell'intestazione corrisponda al contenuto della parte del corpo del messaggio o dei dati dell'entità. Se la parola chiave non corrisponde, il comando verifica il tipo di contenuto del messaggio di risposta confrontandolo con il valore del campo accettato del messaggio di richiesta. È possibile applicare l'azione Consenti o Reimposta a una richiesta o risposta che corrisponde ai criteri della mappa di classe. L'aggiunta dell'azione log determina il messaggio syslog appropriato:
  ```
  APPFW-4- HTTP_CONT_TYPE_VIOLATION
  APPFW-4- HTTP_CONT_TYPE_MISMATCH
  APPFW-4- HTTP_CONT_TYPE_UNKNOWN
  ```
  Utilizzo comando:
  ```
  match {request|response|req-resp} header content-type [mismatch|unknown|violation]
  ```
  Esempio di caso di utilizzoConfigurare un criterio appfw http per bloccare una sessione http che trasporta richieste e risposte con un tipo di contenuto sconosciuto.
  ```
  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
  ```

Ispezione relativa all'utilizzo improprio della porta: questo comando viene utilizzato per impedire l'utilizzo improprio della porta http (80) per altre applicazioni quali IM, P2P, Tunneling e così via. È possibile applicare un'azione Consenti o Reimposta a una richiesta o a una risposta che soddisfa i criteri della mappa di classe. L'aggiunta dell'azione log determina il messaggio syslog appropriato:

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

Utilizzo comando:

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

Esempio di caso di utilizzo

Configurare un criterio AppFw HTTP per bloccare una sessione HTTP utilizzata in modo non corretto per un'applicazione IM.

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

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

- Ispezione Strict-http: questo comando abilita il controllo rigoroso della conformità del protocollo rispetto alle richieste e alle risposte HTTP. È possibile applicare l'azione Consenti o Reimposta a una richiesta o risposta che corrisponde ai criteri della mappa di classe. L'aggiunta dell'azione log causa un messaggio syslog:
  ```
  APPFW-4- HTTP_PROTOCOL_VIOLATION
  ```
  Utilizzo comando:
  ```
  match req-resp protocol-violation
  ```

Esempio di caso di utilizzoConfigurare un criterio http appfw per bloccare le richieste o le risposte che violano la 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
```

- Trasferisci - Ispezione codifica - Questo comando consente di autorizzare, negare o monitorare richieste/risposte il cui tipo di codifica di trasferimento corrisponde al tipo configurato. È possibile applicare l'azione Consenti o Reimposta a una richiesta o risposta che corrisponde ai criteri della mappa di classe. L'aggiunta dell'azione log causa un messaggio syslog:

  ```
  APPFW-6- HTTP_TRANSFER_ENCODING
  ```

  Utilizzo comando:

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

  Esempio di caso di utilizzoConfigurare un criterio http appfw per bloccare una richiesta o una risposta con codifica compress type.

  ```
  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
  ```

- Ispezione applet Java: questo comando verifica se una risposta dispone di un'applet Java e applica l'azione configurata al rilevamento dell'applet. È possibile applicare l'azione Consenti o Reimposta a una richiesta o risposta che corrisponde ai criteri della mappa di classe. L'aggiunta dell'azione log causa un messaggio syslog:

  ```
  APPFW-4- HTTP_JAVA_APPLET
  ```

  Utilizzo comando:

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

  Esempio di caso di utilizzoConfigurare un criterio http appfw per bloccare le applet java.

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

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

Supporto ZFW per messaggistica immediata e controllo delle applicazioni peer-to-peer

Il software Cisco IOS versione 12.4(9)T ha introdotto il supporto ZFW per le applicazioni IM e P2P.

Il software Cisco IOS ha dapprima offerto supporto per il controllo delle applicazioni IM nel software Cisco IOS versione 12.4(4)T. La versione iniziale di ZFW non supportava IM Application nell'interfaccia ZFW. Se si desiderava il controllo delle applicazioni IM, gli utenti non potevano migrare all'interfaccia di configurazione ZFW. Il software Cisco IOS versione 12.4(9)T introduce il supporto ZFW per IM Inspection, che supporta Yahoo! Messenger (YM), MSN Messenger (MSN) e AOL Instant Messenger (AIM). Il software Cisco IOS versione 12.4(9)T è la prima versione del software Cisco IOS a offrire supporto nativo di Cisco IOS Firewall per applicazioni di condivisione file P2P.

Sia l'ispezione IM che P2P offrono criteri Layer 4 e Layer 7 per il traffico delle applicazioni. Ciò significa che ZFW può fornire un'ispezione stateful di base per autorizzare o negare il traffico, così come un controllo granulare di layer 7 su attività specifiche nei vari protocolli, in modo che alcune attività dell'applicazione siano consentite mentre altre vengono negate.

Controllo e ispezione delle applicazioni P2P

SDM 2.2 ha introdotto il controllo dell'applicazione P2P nella sezione di configurazione del firewall. SDM ha applicato un criterio NBAR (Network-Based Application Recognition) e QoS per rilevare e controllare l'attività dell'applicazione P2P a una velocità di linea pari a zero e bloccare tutto il traffico P2P. Ciò ha sollevato il problema che gli utenti CLI, che prevedevano il supporto P2P nella CLI di Cisco IOS Firewall, non erano in grado di configurare il blocco P2P nella CLI a meno che non fossero a conoscenza della necessaria configurazione NBAR/QoS. Il software Cisco IOS versione 12.4(9)T introduce il controllo P2P nativo nella CLI di ZFW, per utilizzare NBAR per rilevare l'attività dell'applicazione P2P. Questa versione del software supporta diversi protocolli applicativi P2P:

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

Le applicazioni P2P sono particolarmente difficili da rilevare, a causa del comportamento di "port-hopping" e di altri trucchi per evitare il rilevamento, così come i problemi introdotti da frequenti modifiche e aggiornamenti alle applicazioni P2P che modificano i comportamenti dei protocolli. ZFW combina l'ispezione stateful del firewall nativo con le funzionalità di riconoscimento del traffico di NBAR per fornire il controllo delle applicazioni P2P nell'interfaccia di configurazione CPL di ZFW. NBAR offre due eccellenti vantaggi:

- Riconoscimento delle applicazioni basato su euristica opzionale per riconoscere le applicazioni nonostante un comportamento complesso e difficile da rilevare
- Infrastruttura estendibile che offre un meccanismo di aggiornamento per rimanere al passo con gli aggiornamenti e le modifiche del protocollo

Configura ispezione P2P

Come accennato in precedenza, l'ispezione e il controllo P2P offrono sia l'ispezione stateful Layer 4 che il controllo delle applicazioni Layer 7. L'ispezione di layer 4 è configurata in modo simile ad altri servizi dell'applicazione, se l'ispezione delle porte native del servizio dell'applicazione è adeguata:

```
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]
```

Si noti l'opzione di firma aggiuntiva nel protocollo di corrispondenza [service-name]. Quando l'opzione di firma viene aggiunta alla fine dell'istruzione del protocollo di corrispondenza, l'euristica

NBAR viene applicata al traffico per cercare le tabelle nel traffico che indicano l'attività specifica dell'applicazione P2P. Ciò include il port-hopping e altri cambiamenti nel comportamento dell'applicazione per evitare il rilevamento del traffico. Questo livello di ispezione del traffico ha il prezzo di un maggiore utilizzo della CPU e di una capacità di throughput di rete ridotta. Se l'opzione di firma non viene applicata, l'analisi euristica basata su NBAR non viene applicata per rilevare il comportamento di salto delle porte e l'utilizzo della CPU non viene influenzato nella stessa misura.

L'ispezione nativa del servizio comporta lo svantaggio di non essere in grado di mantenere il controllo sulle applicazioni P2P nel caso in cui l'applicazione esegua un "hop" su una porta di origine e di destinazione non standard o se l'applicazione viene aggiornata per iniziare l'azione su un numero di porta non riconosciuto:

Applicazione	Porte native (riconosciute dall'elenco 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	Dipendente da PAM
winmx	TCP 6699

Se si desidera consentire (ispezionare) il traffico P2P, è necessario fornire una configurazione aggiuntiva. Alcune applicazioni possono utilizzare più reti P2P o implementare comportamenti specifici che possono essere necessari nella configurazione del firewall per consentire il funzionamento dell'applicazione:

- I client BitTorrent in genere comunicano con i "trackers" (server di directory peer) tramite http che vengono eseguiti su alcune porte non standard. Si tratta in genere di TCP 6969, ma può essere necessario controllare la porta tracker specifica del torrent. Se si desidera consentire BitTorrent, il metodo migliore per supportare la porta aggiuntiva è configurare HTTP come uno dei protocolli di corrispondenza e aggiungere TCP 6969 a HTTP con il comando ip port-map:
  `ip port-map http port tcp 6969`

  Ènecessario definire http e bittorrent come criteri di corrispondenza applicati nella mappa classi.
- eDonkey sembra avviare le connessioni che vengono rilevate sia come eDonkey che come Gnutella.
- L'ispezione KaZaA dipende interamente dal rilevamento della firma NBAR.

L'ispezione di livello 7 (applicazione) aumenta l'ispezione di livello 4 con la capacità di riconoscere e applicare azioni specifiche del servizio, ad esempio bloccare o consentire selettivamente le funzionalità di ricerca file, trasferimento file e chat di testo. Le funzionalità specifiche dei servizi variano a seconda del servizio.

L'ispezione delle applicazioni P2P è simile all'ispezione delle applicazioni 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
```

L'ispezione delle applicazioni P2P offre funzionalità specifiche per un sottoinsieme delle applicazioni supportate dall'ispezione di layer 4:

- edonkey
- fasttrack
- gnutella
- kazaa2

Ognuna di queste applicazioni offre opzioni di criteri di corrispondenza specifici per le applicazioni variabili:

edonkey

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

fasttrack

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

gnutella

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

kazaa2

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

Èpossibile caricare nuove definizioni di protocollo P2P o aggiornamenti dei protocolli P2P correnti con la funzionalità di aggiornamento dinamico pdlm di NBAR. Questo è il comando di configurazione per caricare il nuovo PDLM:

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

Il nuovo protocollo è disponibile nei comandi di protocollo match per class type inspect. Se il nuovo protocollo P2P dispone di servizi (sottoprotocolli), saranno disponibili i nuovi tipi di mappa di classe di ispezione di layer 7 e i criteri di corrispondenza di layer 7.

Ispezione e controllo delle applicazioni IM

Il software Cisco IOS versione 12.4(4)T ha introdotto l'ispezione e il controllo delle applicazioni IM. Il supporto IM non è stato introdotto con ZFW nella versione 12.4(6)T, quindi gli utenti non sono stati in grado di applicare il controllo IM e ZFW nella stessa policy firewall, poiché ZFW e le funzionalità firewall legacy non possono coesistere su una determinata interfaccia.

Il software Cisco IOS versione 12.4(9)T supporta l'ispezione con stato e il controllo delle applicazioni per i seguenti servizi di messaggistica istantanea:

- AOL Instant Messenger
- MSN Messenger
- Yahoo! Messenger

L'ispezione IM è leggermente diversa dalla maggior parte dei servizi, in quanto controlla l'accesso a un gruppo specifico di host per ciascun servizio. I servizi di messaggistica immediata si basano generalmente su un gruppo relativamente permanente di server di elenchi in linea, che i client devono essere in grado di contattare per accedere al servizio di messaggistica immediata. Le applicazioni di messaggistica istantanea tendono ad essere molto difficili da controllare dal punto di vista del protocollo o del servizio. Il modo più efficace per controllare queste applicazioni è quello di limitare l'accesso ai server IM fissi.

Configura ispezione messaggistica immediata

L'ispezione e il controllo dei messaggi istantanei offrono sia l'ispezione stateful Layer 4

e il controllo delle applicazioni di layer 7.

L'ispezione di layer 4 è configurata in modo simile ad altri servizi applicativi:

```
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
```

Le applicazioni IM sono in grado di contattare i server su più porte per mantenerne le funzionalità. Per consentire a un determinato servizio di messaggistica immediata di eseguire l'ispezione, non è necessario un elenco di server per definire l'accesso consentito ai server del servizio di messaggistica immediata. Tuttavia, quando si configura una mappa delle classi che specifica un determinato servizio IM, ad esempio AOL Instant Messenger, e si applica l'azione di eliminazione nella mappa dei criteri associata, il client IM può tentare di individuare una porta diversa per la connessione a Internet. Se non si desidera consentire la connettività a un determinato servizio o se si desidera limitare la funzionalità del servizio di messaggistica immediata alla chat di testo, è necessario definire un elenco di server in modo che ZFW possa identificare il traffico associato

all'applicazione di messaggistica immediata:

```
!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
```

Ad esempio, l'elenco dei server di messaggistica immediata di Yahoo è definito come segue:

```
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
```

Ènecessario applicare l'elenco dei server alla definizione del protocollo:

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

Per abilitare la risoluzione dei nomi, è necessario configurare i comandi ip domain lookup e ip name-server ip.ad.re.ss.

I nomi dei server di messaggistica immediata sono piuttosto dinamici. È necessario verificare periodicamente che gli elenchi dei server di messaggistica immediata configurati siano completi e corretti.

L'ispezione di livello 7 (applicazione) migliora l'ispezione di livello 4 con la capacità di riconoscere e applicare azioni specifiche del servizio, ad esempio bloccare o consentire selettivamente funzionalità di chat di testo e negare altre funzionalità del servizio.

Ispezione delle applicazioni IM offre attualmente la possibilità di distinguere tra l'attività di chat di testo e tutti gli altri servizi applicativi. Per limitare l'attività di messaggistica istantanea alla chat di testo, configurare un criterio di livello 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]
```

Applica il criterio Layer 7 a Yahoo! Criteri di Messenger configurati in precedenza:

```
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
```

Filtri URL

ZFW offre funzionalità di filtro URL per limitare l'accesso al contenuto Web a quello specificato da una lista bianca o nera definita sul router, o inoltrando i nomi di dominio a un server di filtro URL per verificare l'accesso a domini specifici. Il filtro URL ZFW nel software Cisco IOS versione 12.4(6)T - 12.4(15)T viene applicato come un'ulteriore azione policy, simile all'ispezione delle applicazioni.

Per il filtro URL basato sul server, è necessario definire una mappa dei parametri che descriva la configurazione del server urlfilter:

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

Se si preferisce l'uso di liste bianche o nere statiche, è possibile definire un elenco di domini o sottodomini che sono esplicitamente autorizzati o rifiutati, mentre l'azione inversa viene applicata al traffico che non corrisponde all'elenco:

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

Se nelle definizioni di dominio esclusivo è stata definita una lista nera di URL con opzioni di negazione, sono consentiti tutti gli altri domini. Se vengono definite delle definizioni di "permesso", tutti i domini autorizzati devono essere specificati esplicitamente, in modo simile alla funzione degli elenchi di controllo degli accessi IP.

Impostare una mappa delle classi che corrisponda al traffico HTTP:

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

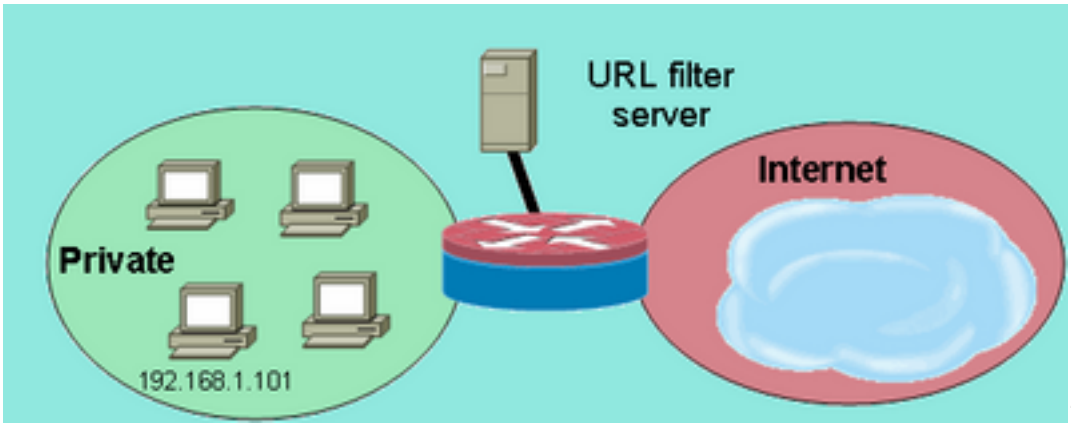
Definire una mappa dei criteri che associ la mappa delle classi alle operazioni inspect e urlfilter:

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

In questo modo viene configurato il requisito minimo per la comunicazione con un server filtro URL. Sono disponibili diverse opzioni per definire un comportamento aggiuntivo del filtro URL.

Alcune distribuzioni di rete desiderano applicare il filtro URL per alcuni host o subnet e ignorare il filtro URL per altri host. Ad esempio, nella Figura 9, per tutti gli host nella zona privata il traffico HTTP deve essere controllato da un server filtro URL, ad eccezione dell'host specifico 192.168.1.101.

Figura 10: Topologia di esempio del filtro URL



Topologia di esempio del filtro URL

A tale scopo, è possibile definire due diverse mappe di classi:

- Una class-map che corrisponde solo al traffico HTTP per il gruppo più ampio di host che ricevono il filtro URL.
- Una class-map per il gruppo più piccolo di host che non ricevono il filtro URL. La seconda mappa di classe corrisponde al traffico HTTP e a una lista di host esentati dai criteri di filtro URL.

Entrambe le mappe di classe sono configurate in una mappa dei criteri, ma solo una riceve l'operazione 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
```

Controllo dell'accesso al router

La maggior parte dei tecnici della sicurezza di rete si sente a disagio se espone le interfacce di gestione del router (ad esempio SSH, Telnet, HTTP, HTTPS, SNMP e così via) alla rete Internet pubblica e, in determinate circostanze, il controllo è necessario anche per l'accesso LAN al router. Il software Cisco IOS offre una serie di opzioni per limitare l'accesso alle varie interfacce, tra cui la famiglia di funzionalità Network Foundation Protection (NFP), vari meccanismi di controllo dell'accesso per le interfacce di gestione e l'area autonoma di ZFW. È necessario esaminare altre funzionalità, ad esempio il controllo degli accessi VTY, la protezione del piano di gestione e il controllo degli accessi SNMP, per determinare la combinazione di funzionalità di controllo del router più adatta per l'applicazione specifica.

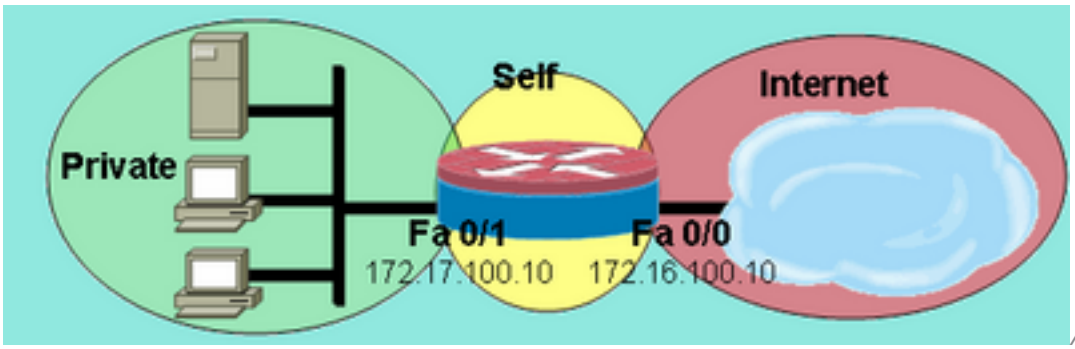
In genere, la famiglia di funzionalità NFP è più adatta per il controllo del traffico destinato al router stesso. Per informazioni sulla protezione del router con le funzionalità NFP, fare riferimento alla panoramica della protezione del Control Plane nel software Cisco IOS.

Se si decide di applicare il protocollo ZFW per controllare il traffico da e verso gli indirizzi IP del router, è necessario comprendere che le policy e le funzionalità predefinite del firewall sono diverse da quelle disponibili per il traffico di transito. Il traffico di transito è definito come traffico di rete i cui indirizzi IP di origine e di destinazione non corrispondono ad alcun indirizzo IP applicato ad alcuna delle interfacce del router e il traffico non causa l'invio da parte del router di messaggi di controllo di rete, ad esempio scadenza TTL ICMP o messaggi rete/host non raggiungibili.

Lo ZFW applica una policy di negazione totale predefinita al traffico che si sposta tra le zone, ad eccezione del fatto che, come accennato nelle regole generali, il traffico in qualsiasi zona che fluisce direttamente agli indirizzi delle interfacce del router è consentito in modo implicito. In questo modo si garantisce che la connettività alle interfacce di gestione del router venga mantenuta quando al router viene applicata una configurazione del firewall per una zona. Se lo stesso criterio di negazione di tutto influisce direttamente sulla connettività al router, è necessario applicare una configurazione completa del criterio di gestione prima di configurare le zone sul router. Ciò potrebbe compromettere la connettività di gestione se i criteri non vengono implementati o applicati correttamente.

Quando un'interfaccia è configurata come membro della zona, gli host connessi all'interfaccia vengono inclusi nella zona. Tuttavia, il traffico che scorre da e verso gli indirizzi IP delle interfacce del router non è controllato dalle policy di zona (ad eccezione delle circostanze descritte nella nota della Figura 10). Al contrario, quando si configura lo ZFW, tutte le interfacce IP sul router vengono automaticamente integrate nella zona automatica. Per controllare il traffico IP che si sposta sulle interfacce del router dalle varie zone di un router, è necessario applicare le policy di blocco o autorizzazione/ispezione del traffico tra la zona e l'area autonoma del router e viceversa (vedere la Figura 11).

Figura 11: Applicazione dei criteri tra le aree di rete e l'area autonoma del router



Applicazione dei criteri tra le aree di rete e l'area autonoma del router

Sebbene il router offra un criterio di autorizzazione predefinito tra tutte le zone e l'area autonoma, se un criterio è configurato da una qualsiasi zona all'area autonoma e nessun criterio è configurato dall'utente alle zone connesse all'interfaccia configurabili dall'utente del router, tutto il traffico originato dal router incontra il criterio da zona connessa a area autonoma al suo ritorno sul router e viene bloccato. Pertanto, il traffico originato dal router deve essere ispezionato per consentirne il ritorno alla zona di origine.

> **Nota:** Il software Cisco IOS utilizza sempre l'indirizzo IP associato agli host di destinazione "più vicini" dell'interfaccia per il traffico, ad esempio syslog, tftp, telnet e altri servizi del control-plane, e assoggetta il traffico ai criteri del firewall per l'area automatica. Tuttavia, se un servizio definisce un'interfaccia specifica come interfaccia-origine con comandi che includono, tra l'altro, la registrazione dell'interfaccia-origine [tipo numero] , l'interfaccia-origine ip tftp [tipo numero] e l'interfaccia-origine ip telnet [tipo numero], il traffico viene sottoposto all'area autonoma.

Nota:alcuni servizi (in particolare i servizi Voice over IP dei router) utilizzano interfacce temporanee o non configurabili che non possono essere assegnate alle aree di sicurezza. Questi servizi non possono funzionare correttamente se il traffico non può essere associato a un'area di sicurezza configurata.

Limitazioni dei criteri di area autonoma

I criteri di area autonoma hanno funzionalità limitate rispetto ai criteri disponibili per coppie di zone traffico di transito:

- Come nel caso dell'ispezione stateful classica, il traffico generato dal router è limitato a TCP, UDP, ICMP e all'ispezione di protocolli complessi per H.323.
- Controllo applicazione non disponibile per i criteri di tipo self-zone.
- Impossibile configurare la limitazione della sessione e della velocità in criteri di zona autonomi.

Configurazione criteri area autonoma

Nella maggior parte dei casi si tratta di policy di accesso auspicabili per i servizi di gestione dei router:

- Nega tutta la connettività Telnet, poiché il protocollo non crittografato di Telnet espone facilmente le credenziali utente e altre informazioni riservate.
- Consente le connessioni SSH da qualsiasi utente in qualsiasi zona. SSH cripta le credenziali dell'utente e i dati della sessione, fornendo protezione da utenti malintenzionati che utilizzano strumenti di acquisizione dei pacchetti per intercettare l'attività dell'utente e compromettere le credenziali dell'utente o le informazioni riservate, ad esempio la configurazione del router. SSH versione 2 offre una protezione più avanzata e risolve le vulnerabilità specifiche inerenti a SSH versione 1.
- Consenti connettività HTTP al router dalle zone private se la zona privata è attendibile. In caso contrario, se nella zona privata è possibile che utenti malintenzionati compromettano le informazioni, HTTP non utilizza la crittografia per proteggere il traffico di gestione e può rivelare informazioni riservate, quali le credenziali utente o la configurazione.
- Consenti connettività HTTPS da qualsiasi zona. Analogamente a SSH, HTTPS crittografa i dati della sessione e le credenziali dell'utente.
- Limitare l'accesso SNMP a un host o a una subnet specifici. L'SNMP può essere utilizzato per modificare la configurazione del router e rivelare le informazioni di configurazione. L'SNMP deve essere configurato con il controllo dell'accesso sulle varie community.
- Blocca le richieste ICMP da Internet pubblica all'indirizzo della zona privata (presumendo che l'indirizzo della zona privata sia instradabile). Se necessario, è possibile esporre uno o più indirizzi pubblici al traffico ICMP per la risoluzione dei problemi di rete. È possibile utilizzare diversi attacchi ICMP per sovraccaricare le risorse del router o per ripristinare la topologia e l'architettura della rete.

Un router può applicare questo tipo di criterio aggiungendo due coppie di zone per ogni zona da controllare. Ogni coppia di zone per il traffico in entrata o in uscita dalla zona autonoma del router deve corrispondere ai rispettivi criteri nella direzione opposta, a meno che il traffico non abbia origine nella direzione opposta. È possibile applicare una mappa dei criteri per ogni coppia di zone in entrata e in uscita che descrive tutto il traffico oppure è possibile applicare mappe dei criteri

specifiche per ogni coppia di zone. La configurazione di coppie di zone specifiche per mappa dei criteri fornisce la granularità necessaria per visualizzare l'attività corrispondente a ogni mappa dei criteri.

Un esempio di rete con una stazione di gestione SNMP a 172.17.100.11 e un server TFTP a 172.17.100.17, questo output fornisce un esempio dell'intera policy di accesso all'interfaccia di gestione:

```
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
```

Sfortunatamente, la policy di zona non offre la possibilità di ispezionare i trasferimenti TFTP. Pertanto, se il protocollo TFTP deve passare attraverso il firewall, il firewall deve trasmettere tutto il traffico da e verso il server TFTP.

Se il router termina le connessioni VPN IPSec, è necessario definire anche un criterio per passare IPSec ESP, IPSec AH, ISAKMP e IPSec NAT-T (UDP 4500). A seconda dei servizi che si utilizzano. Questo criterio successivo può essere applicato in aggiunta al criterio precedente. Si noti la modifica alle mappe dei criteri in cui è stata inserita una mappa delle classi per il traffico VPN con un'azione di passaggio. In genere, il traffico crittografato è attendibile, a meno che il criterio di sicurezza non indichi che è necessario consentire il traffico crittografato da e verso gli endpoint specificati.

```
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
```

Servizi firewall basati su zone e applicazioni ad ampio raggio

Per una nota sull'applicazione che fornisce esempi di configurazione e guide per l'utilizzo, consultare la nota sulla versione per i servizi delle applicazioni Cisco Wide Area (Software versione 4.0.13) - Nuove funzionalità della versione software 4.0.13

Monitorare il firewall dei criteri basato su zone con i comandi show e debug

ZFW introduce nuovi comandi per visualizzare la configurazione delle policy e monitorare l'attività del firewall.

Visualizza la descrizione della zona e le interfacce contenute in una zona specificata:

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

Quando il nome della zona non è incluso, il comando visualizza le informazioni di tutte le zone configurate.

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

Visualizza la zona di origine, la zona di destinazione e il criterio collegati alla coppia di zone:

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

Se non si specifica alcuna origine o destinazione, vengono visualizzate tutte le coppie di zone con origine, destinazione e il criterio associato. Quando viene indicata solo la zona di origine/destinazione, vengono visualizzate tutte le coppie di zone che contengono questa zona come origine/destinazione.

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

Visualizza una mappa dei criteri specificata:

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

Quando il nome di una mappa dei criteri non viene specificato, vengono visualizzate tutte le mappe dei criteri di tipo inspect, insieme alle mappe dei criteri di livello 7 contenenti un sottotipo.

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

Visualizza le statistiche della mappa dei criteri del tipo di controllo in fase di esecuzione attualmente su una coppia di zone specificata.

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

Quando non viene indicato alcun nome di coppia di zone, vengono visualizzate le mappe dei criteri su tutte le coppie di zone.

L'opzione sessioni visualizza le sessioni di ispezione create dall'applicazione di mappa dei criteri sulla coppia di zone specificata.

```
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
```

La parola chiave urlfilter visualizza le statistiche relative all'oggetto urlfilter relative alla mappa dei criteri specificata (o alle mappe dei criteri su tutte le destinazioni quando non è specificato alcun nome di coppia di zone):

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

Quando si specifica la parola chiave cache insieme a urlfilter , viene visualizzata la cache urlfilter (di indirizzi IP).

Riepilogo del comando show policy-map per ispezionare le policy-map:

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

Ottimizzazione della protezione da attacchi Denial of Service del firewall dei criteri basati su zone

ZFW offre la protezione DoS per avvisare i tecnici di rete di cambiamenti significativi nelle attività di rete e per mitigare le attività indesiderate per ridurre l'impatto delle modifiche delle attività di rete. ZFW mantiene un contatore separato per ogni mappa delle classi della mappa dei criteri. Pertanto, se si utilizza una mappa di classe per le mappe dei criteri di due coppie di zone diverse, vengono applicati due diversi set di contatori di protezione DoS.

ZFW fornisce la riduzione degli attacchi DoS come impostazione predefinita nelle versioni software Cisco IOS precedenti alla 12.4(11)T. Il comportamento predefinito della protezione DoS è stato modificato nel software Cisco IOS versione 12.4(11)T.

Per ulteriori informazioni sugli attacchi DoS SYN di TCP, fare riferimento a Definizione delle strategie di protezione dagli attacchi Denial of Service della rete SYN TCP.

Appendici

Appendice A Configurazione di base

```
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
```

Appendice B Configurazione finale (completa)

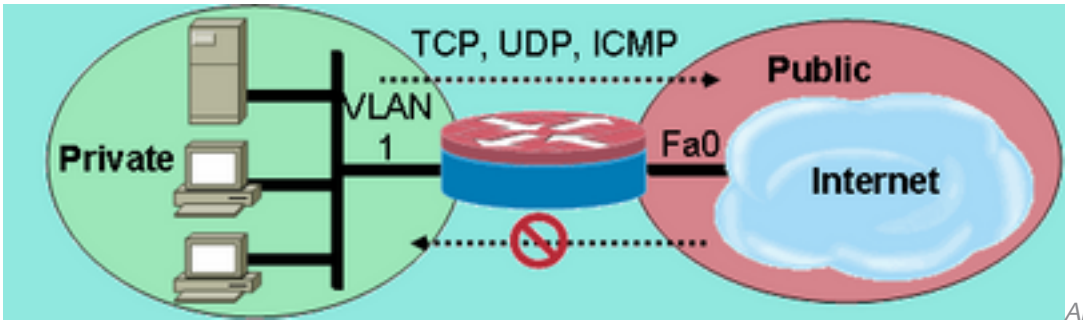
```
ip subnet-zero
ip cef
!
ip port-map user-Xwindows port tcp from 6900 to 6910
!
class-map type inspect match-any L4-inspect-class
 match protocol tcp
 match protocol udp
 match protocol icmp
class-map type inspect match-any L7-inspect-class
  match protocol ssh
  match protocol ftp
  match protocol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

```
  service-policy type inspect private-internet-policy
zone-pair security servers-clients source servers destination clients
  service-policy type inspect servers-clients-policy
zone-pair security clients-servers source clients destination servers
  service-policy type inspect clients-servers-policy
zone-pair security private-dmz source private destination dmz
  service-policy type inspect private-dmz-policy
zone-pair security internet-dmz source internet destination dmz
  service-policy type inspect internet-dmz-policy
!
bridge irb
!
interface FastEthernet0
 ip address 172.16.1.88 255.255.255.0
 zone-member internet
!
interface FastEthernet1
 ip address 172.16.2.1 255.255.255.0
 zone-member dmz
!
interface FastEthernet2
 switchport access vlan 2
!
interface FastEthernet3
 switchport access vlan 2
!
interface FastEthernet4
 switchport access vlan 1
!
interface FastEthernet5
 switchport access vlan 1
!
interface FastEthernet6
 switchport access vlan 1
!
interface FastEthernet7
 switchport access vlan 1
!
interface Vlan1
 no ip address
 zone-member clients
 bridge-group 1
!
interface Vlan2
 no ip address
 zone-member servers
 bridge-group 1
!
interface BVI1
 ip address 192.168.1.254 255.255.255.0
 zone-member private
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.16.1.1
!
access-list 110 permit ip any host 172.16.2.2
access-list 111 permit ip any host 172.16.2.3
!
bridge 1 protocol ieee
bridge 1 route ip
!
End
```

Appendice C: Configurazione di base del firewall per i criteri di zona per due zone

Nell'esempio viene fornita una semplice configurazione come base per testare le funzionalità per migliorare il software Cisco IOS ZFW. Questa configurazione è una configurazione modello per due zone, come configurata su un router 1811. La zona privata viene applicata alle porte fisse dello switch del router, in modo che tutti gli host sulle porte dello switch siano connessi alla VLAN 1. La zona pubblica viene applicata alla rete Fast Ethernet 0 (vedere Figura 12).

Figura 12: Area pubblica applicata su Fast Ethernet 0



Area pubblica applicata su Fast Ethernet 0

```
class-map type inspect match-any private-allowed-class
 match protocol tcp
 match protocol udp
 match protocol icmp
class-map type inspect match-all http-class
 match protocol http
!
policy-map type inspect private-allowed-policy
 class type inspect http-class
  inspect my-parameters
 class type inspect private-allowed-class
  inspect
!
zone security private
zone security public
zone-pair security priv-pub source private destination public
 service-policy type inspect private-allowed-policy
!
interface fastethernet 0
 zone-member security public
!
interface VLAN 1
 zone-member security private
```

Informazioni correlate

- Documentazione e supporto tecnico – Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).