Cisco Router Security

Francesco Palmieri
fpalmier@unina.it

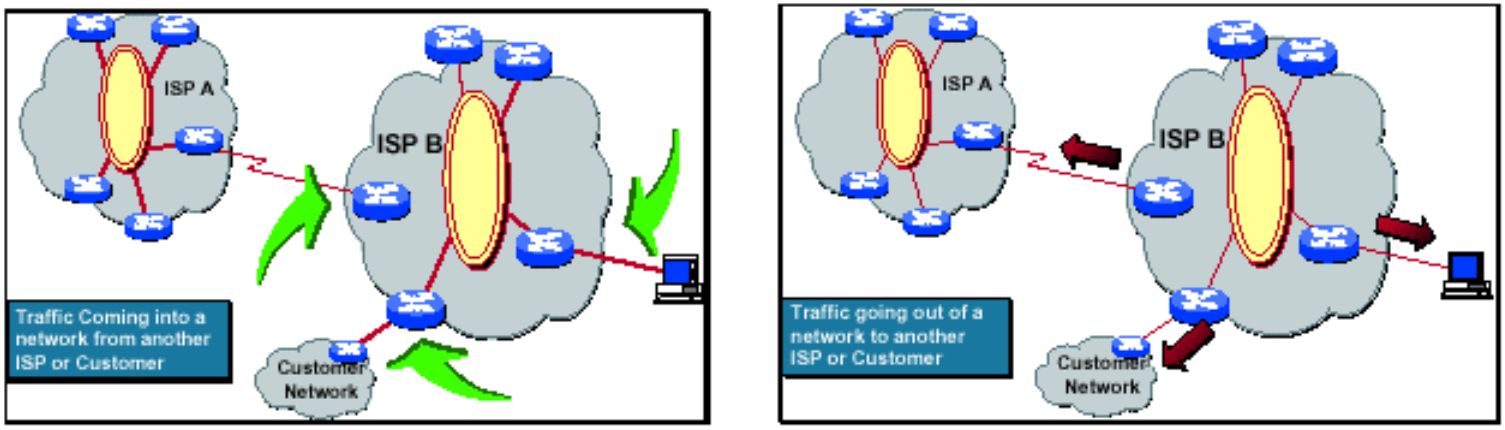
Cisco Router Security

- Generalità
- Accesso diretto al router
- Accessi in-band SNMP/HTTP
- Filtri sul traffico
- Denial Of Service
- Logging/Auditing

Generalità

- Generalmente il border router è il primo sbarramento di difesa della propria rete
- E’ uno strumento estremamente flessibile e specializzato in ambito networking e offre quindi un novero di opzioni e funzionalità che nessuna macchina general-purpose può garantire
- Permette di centralizzare il controllo di un considerevole numero di aspetti relativi alla security
- Offre un framework completo per la gestione e il trattamento in sicurezza dei flussi di traffico entranti e uscenti dalla propria rete

Obiettivo:
Garanzie di sicurezza su traffico entrante e uscente



Accesso diretto - Password Security

- Tutte le password sono conservate in chiaro a meno di non attivare esplicitamente il servizio di cifratura delle password:

  service password-encryption

- La cifratura è facilmente invertibile, essendo basata su uno schema di Vigenerè quindi una configurazione contenente password cifrate va trattata con la medesima cura di una con tutte le password in chiaro

Accesso diretto - Password Security

- Per la password di accesso privilegiato è possibile utilizzare uno schema meno debole basato sull'hashing MD5. Quindi invece del consueto comando

  enable password mypass

  è opportuno impostare la password di accesso privilegiato con:

  enable secret mypass

Accesso diretto - login

- Tutti gli accessi diretti attraverso le interfacce asincrone (console e aux) o attraverso le interfacce di rete (vty) devono essere controllati e protetti con password

```
line console 0
login
password 1stAccessKey

line aux 0
login
password 2ndAccessKey
```

Accesso diretto - login

- E’ bene autenticare gli accessi al router tramite coppie user/passwd localmente definite

```
username user1 password 7 013764351542
line vty 0 4
    login local
```

- E’ancora meglio ove possibile prevedere un’ autenticazione esterna RADIUS o TACACS+

```
aaa new-model
aaa authentication login default tacacs+ enable
aaa authentication login netstaff local enable
tacacs-server host 192.132.34.41
```

Accesso Diretto - async

- E’ possibile stabilire una connessione a un’interfaccia asincrona attraverso la rete attraverso il meccanismo del “*reverse telnet*”
- Tale funzionalità è disabilitabile applicando a ciascuna linea il comando:

```
transport input none
```

- o filtrare con un’access list in ingresso:

```
access-list 2 deny any
line aux 0
    access-class 2 in
```

Accesso Diretto - vty

- L’accesso interattivo attraverso la rete deve essere ristretto ai soli host esplicitamente autorizzati tramite ACL

```
access-list 1 permit 192.133.28.100 0.0.0.0
access-list 1 permit 192.133.28.101 0.0.0.0

line vty 0 4
    access-class 1 in
```

Accesso Diretto - vty

- Ogni interfaccia di rete deve ammettere connessioni attraverso i soli protocolli necessari. Ad esempio per accettare solo sessioni telnet

```
line vty 0 4
    transport input telnet
    transport output none
```

oppure telnet ed ssh

```
line vty 0 4
    transport input telnet ssh
    transport output none
```

Accesso Diretto – vty e async

- Per proteggere interfacce asincrone lasciate senza sorveglianza e per evitare denial of service attraverso l'esaurimento del numero di vty disponibili e' possibile impostare un timer di inattività sulle interfacce:

  exec-timeout *min sec*

- Che per evitare il blocco dei vty può essere combinato con l'abilitazione della funzionalità di *TCP keepalive* sulle connessioni entranti:

  service tcp-keepalives-in

Accesso Diretto - Anti-Bouncing

- Per evitare che un router possa essere usato come “trampolino” per connessioni illecite vanno bloccate le sessioni telnet in uscita:

```
access-list 1 deny 0.0.0.0 0.0.0.0
access-list 2 permit 0.0.0.0 255.255.255.255

line vty 0 4
    access-class 1 out
```

e per abilitare il solo utente xyz al telnet uscente:

username *xyz* access-class 2 password *xyzownpassword*

Accesso Diretto - Banner

- E’ consigliabile informare attraverso un banner chi accede dall’esterno circa eventuali restrizioni di acesso, conseguenze penali per l’uso illegale delle risorse, politiche di logging/monitoring degli eventi:

```
banner login ^C
WARNING: Every connection or connection attempt
will be logged for further analysis.
Unauthorized access and resource usage is strongly
prohibited and will be prosecuted as a criminal offence
according to local laws.
^C
```

Identificazione Remota

- E’ possibile abilitare l’identificazione degli utenti remoti di ogni connessione TCP attraverso il protocollo *ident* (RFC 1413), in global configuration mode, tramite il comando:

  ip identd

- Tale protocollo è comunque da considerarsi inerentemente insicuro in termini di affidabilità dei dati forniti

Accesso SNMP - Restrizioni

- L’accesso SNMP in lettura e scrittura deve essere ristretto ai solo hosts autorizzati tramite ACL:

```
access-list 10 permit 192.132.34.45 0.0.0.0
access-list 10 permit 192.132.34.103 0.0.0.0
access-list 11 permit 192.132.34.0 0.0.0.255

snmp-server community mypassword RW 10
snmp-server community notpublic     RO 11
snmp-server tftp-server-list 10
```

- Le communiti strings più ovvie (es. *public* e *private* andrebbero evitate

Accesso SNMP - Community

- Nella versione 1 le community strings viaggiano in chiaro, quindi per evitare il più possibile la loro intercettazione tramite *sniffing/wiretapping* l'autenticazione dei traps andrebbe disabilitata:

```
! define the hosts receiving SNMP traps
snmp-server host 192.132.34.103 secretkey
! disable trap authentication via community
no snmp-server trap-authentication
```

- L'autentificazione dei traps va abilitata solo nella versione 2 di SNMP

Accesso SNMP – Versione 2

- La versione 2 del protocollo che prevede uno schema di digest-authentication basato su MD5 andrebbe usata ovunque possibile:

```
! local MD5-authenticated party
snmp-server party swdep1 initialPartyId.131.108.45.32.4
    packetsize 1500 local authentication md5
    23de457623900ac3ef568fcb236589 lifetime 400
```

- La configurazione specifica di una community string abilita implicitamente anche la versione 1

Accesso HTTP - Restrizioni

- Il meccanismo di in-band management WWW attraverso il protocollo HTTP deve essere ristretto ai soli client autorizzati tramite ACL:

```
access-list 10 permit 192.132.34.45 0.0.0.0
access-list 10 permit 192.132.34.103 0.0.0.0

ip http server
ip http access-class 10
```

Accesso HTTP - Autenticazione

- Tutte le transazioni di HTTP management devono essere autenticate tramite username/password:
  - ***Utenti locali***

    ip http authentication local
  - ***Via Enable password***

    ip http authentication enable
  - ***AAA TACACS+/RADIUS***

    ip http authentication aaa
  - ***TACACS***

    ip http authentication tacacs
- Le password di autenticazione viaggiano in chiaro

Filtri sul traffico - Firewalling

- Allo scopo di proteggere in maniera centralizzata tutti gli hosts accessibili sulle reti interne è consigliabile filtrare selettivamente a livello di border router i servizi tendenzialmente pericolosi:

TCP/53	***DNS xfer***	**UDP/512**	***biff***
UDP/67-68	***bootp***	**UDP/513**	***who***
UDP/69	***TFTP***	**UDP/514**	***syslog***
TCP/79	***finger***	**UDP/520**	***route***
TCP/87	***link***	**TCP/540-541**	***uucp***
TCP-UDP/111	***SUN RPC***	**TCP-UDP/635**	***mountd***
TCP-UDP/137-139	***NetBIOS***	**TCP-UDP/200x**	***openwin***
TCP/144	***NeWS***	**TCP-UDP/2049**	***NFS***
UDP/161-162	***SNMP***	**TCP-UDP/600x**	***X11***
TCP/512-515	***rcmds/lpd***		

Firewalling - blocco

```
access-list 111 deny   udp any any eq bootps log
access-list 111 deny   udp any any eq tftp log
access-list 111 deny   tcp any any eq 87 log
access-list 111 deny   udp any any eq sunrpc log
access-list 111 deny   tcp any any eq sunrpc log
access-list 111 deny   tcp any any eq exec log
access-list 111 deny   tcp any any eq login log
access-list 111 deny   tcp any any eq cmd log
access-list 111 deny   tcp any any eq lpd log
access-list 111 deny   udp any any eq 6000 log
access-list 111 deny   tcp any any eq 6000 log
access-list 111 permit ip any any

! Border interface
interface Serial 0
      ip access-group 111 in
```

Firewalling – controllo selettivo

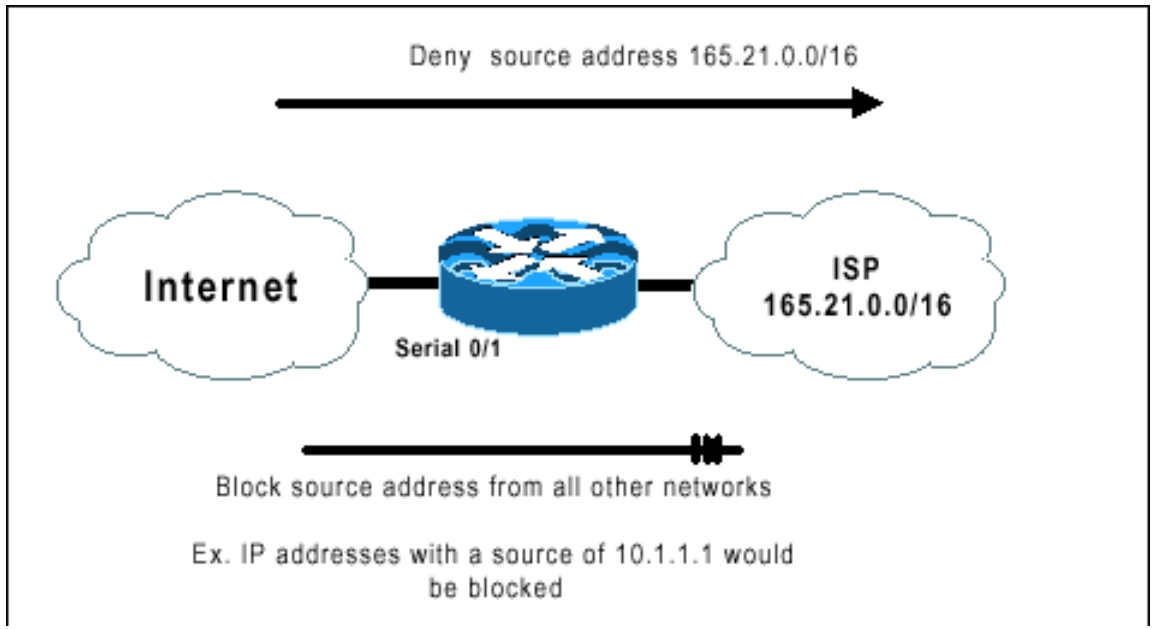
```
! DNS queries only to official servers
access-list 111 permit udp any host dscna1.unina.it eq 53
access-list 111 permit udp any host dscna2.unina.it eq 53
access-list 111 deny udp any any eq 53 log
! Zone-xfer from authorized servers
access-list 111 permit tcp host dns.iuo.it host dscna1.unina.it eq 53
access-list 111 deny tcp any any eq 53 log
! Finger to home server only
access-list 111 permit tcp any host cd.unina.it eq 79
access-list 111 deny   tcp any any eq 162 log
! SNMP queries only from authorized foreign hosts
access-list 111 permit udp host 192.135.23.4 any eq snmp
access-list 111 permit tcp host 192.135.23.4 any eq 162
access-list 111 deny   udp any any eq snmp log
access-list 111 deny   tcp any any eq 162 log
```

Firewalling – Filtri Anti Spam

- Per evitare l'applicazione di esplicite misure anti-spam a livello di tutti gli hosts è conveniente limitare l'accesso SMTP in ingresso ai soli mail-exchangers ufficiali, su cui va concentrata l'applicazione di tutti i meccanismi di protezione

```
Interface  ATM0/0.1 point-to-point
     ip access-group 101 in

access-list 101 permit tcp any host mail.unina.it eq smtp
access-list 101 deny tcp any 143.225.0.0 0.0.255.255 eq smtp log
access-list 101 permit ip any any
```

Filtri sul traffico
Anti Spoofing – Filtro in ingresso



Anti Spoofing – Filtro in ingresso

- Gran parte degli attacchi in rete si basano sulla falsificazione fraudolenta degli indirizzi d'origine. Il modo più semplice di proteggersi è quello di scartare, a livello di border router, tutto il traffico in ingresso con indirizzi sorgente manifestamente inammissibili rispetto alla provenienza:

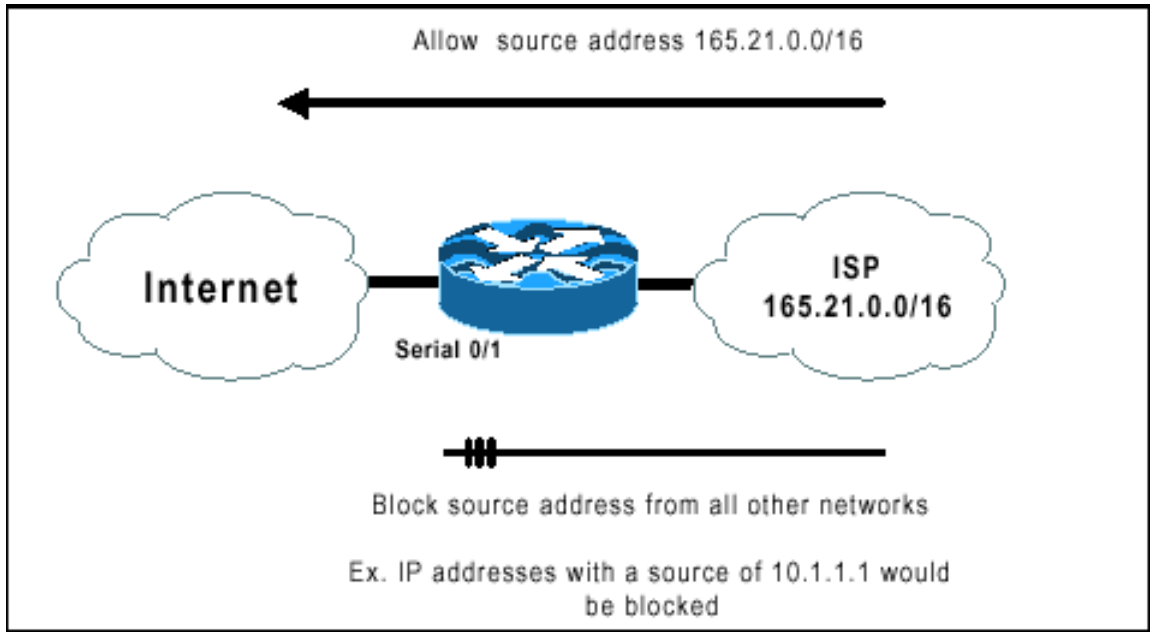
```
! Blocca i traffico dall'esterno con indirizzi sorgente interni
access-list 111 deny   ip 165.21.0.0 0.0.255.255 any log
access-list 111 permit ip any any

interface Serial0/1
   ip access-group 111 in
```

Anti Spoofing – Filtro in ingresso

- E’ opportuno bloccare anche tutto il traffico proveniente dall’esterno con indirizzi sorgente riservati (RFC 1918) o comunque non correttamente instradabili aggiungendo all’ACL in ingresso

```
access-list 101 deny ip host 0.0.0.0 any log
! Incoming with loopback source address
access-list 101 deny ip 127.0.0.0 0.255.255.255 any log
! Incoming with RFC 1918 reserved address
access-list 101 deny ip 10.0.0.0 0.255.255.255 any log
access-list 101 deny ip 172.16.0.0 0.15.255.255 any log
access-list 101 deny ip 192.168.0.0 0.0.255.255 any log
```

Filtri sul traffico
Anti-Spoofing – Filtro in uscita



Anti Spoofing – Filtro in uscita

- Per prevenire inoltre spoofing, volontari o involontari, dall'interno della propria rete verso l'esterno, analoghe misure di filtraggio vanno applicate sul border router in uscita

```
! Blocca il traffico uscente con indirizzi sorgente estranei
access-list 112 permit ip 165.21.0.0 0.0.255.255 any
access-list 112 deny ip any any log

interface Serial0/1
    ip access-group 112 out
```

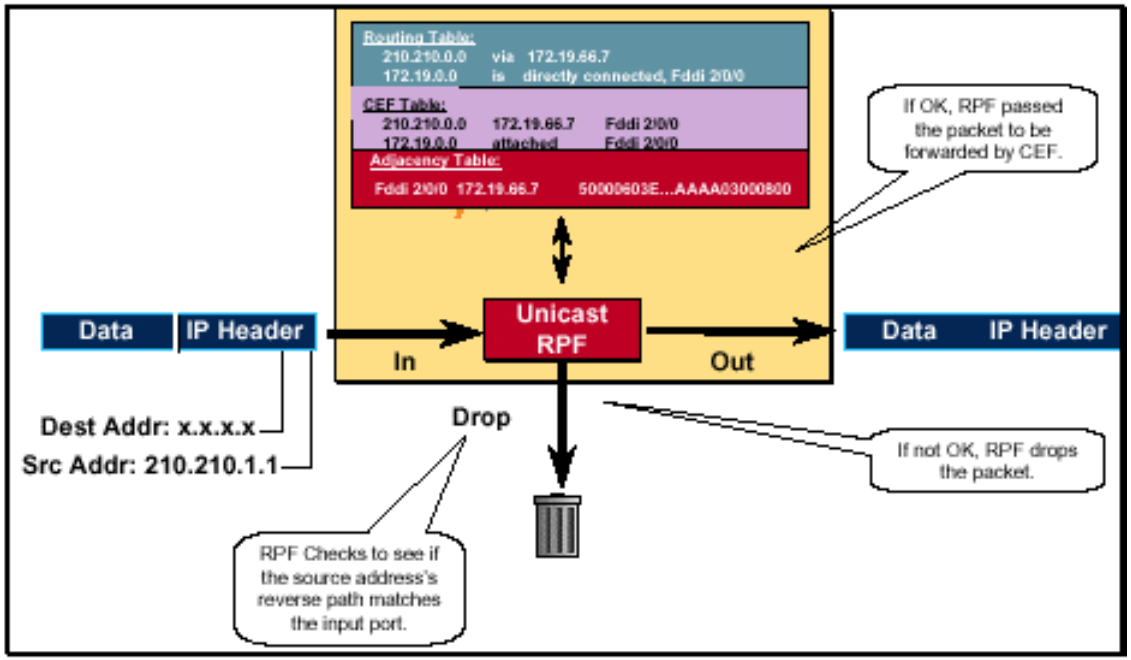
Anti Spoofing – Unicast RPF

- Un modo estremamente elegante ed efficace di inibire lo spoofing è quello di sfruttare la feature di *Unicast Reverse Path Forwarding* (RPF) su versioni IOS basate su *RSP* che supportano la funzionalità di *Cisco Express Forwarding* (CEF). Tale meccanismo è utilizzabile solo in presenza di routing totalmente simmetrico

```
! Enable CEF – with a VIP2 can use “ip cef distributed”
ip cef

int Serial4/0/1
    ip verify unicast reverse-path
```

Anti-Spoofing – Unicast RPF

- Il controllo di ammissibilità per ogni pacchetto è fatto implicitamente in ingresso all'interfaccia. Se all' indirizzo sorgente non è associata una route nella "*CEF table*" che punta a ritroso sulla stessa interfaccia su cui il pacchetto è arrivato esso viene scartato



Integrità del routing – source routing

- Tutta una serie di attacchi tendono ad influenzare i meccanismi di instradamento al fine di effettuare modifiche illecite alla topologia e all'uso delle risorse della rete oppure di perturbarne il funzionamento al solo scopo di denial of service

- Una delle misure di prevenzione basilari è la disabilitazione dei meccanismi di *source routing*

  no ip source-route

Integrità del routing – icmp redirects

- Il meccanismo dell'ICMP redirect, in genere usato per informare le stazioni di una rete locale circa l'uso preferenziale di un router per raggiungere determinate destinazioni può essere utilizzato per corrompere opportunamente dall'esterno le tavole di routing degli hosts di una rete. E' opportuno quindi filtrare i redirects in ingresso e inibire la funzionalità a livello di interfaccia

```
access-list 111 deny icmp any any redirect

interface Serial0/1
    no ip redirects
    ip access-group 111 in
```

Integrità del routing dinamico

- Ove sia previsto lo scambio di informazioni di instradamento attraverso protocolli di routing dinamico, è sempre opportuno, a scopo di garantire l'integrità dei processi di routing da alterazioni dolose, prevedere l'uso di meccanismi di autenticazione dei partecipanti al colloquio.
- I protocolli di routing che attualmente offrono il meccanismo della *neighbor authentication* sono:

BGP *	EIGRP *
DRP SA	OSPF *
IS-IS	RIPv2 *

* = Autenticazione non in chiaro (MD5)

Integrità del routing dinamico

- Per attivare una sessione BGP con autenticazione MD5

```
router bgp 65282
no synchronization
neighbor 193.206.130.5 remote-as 137
neighbor 193.206.130.5 password m1ck5xof43j72
```

- E’ inoltre opportuno non accettare, ne’ inviare nei routing updates classi riservate RFC 1918. È pertanto consigliabile operare meccanismi di filtraggio degli annunci a livello di liste di distribuzione

Integrità del routing dinamico

```
router bgp 65282
no synchronization
neighbor 193.206.130.5 remote-as 137
neighbor 193.206.130.5 distribute-list 107 in
neighbor 193.206.130.5 distribute-list 108 out
no auto-summary

access-list 108 deny ip host 0.0.0.0 any
access-list 108 deny ip 10.0.0.0 0.255.255.255 255.0.0.0 0.255.255.255
access-list 108 deny ip 172.16.0.0 0.15.255.255 255.240.0.0 0.15.255.255
access-list 108 deny ip 192.168.0.0 0.0.255.255 255.255.0.0 0.0.255.255
access-list 108 permit ip any any
```

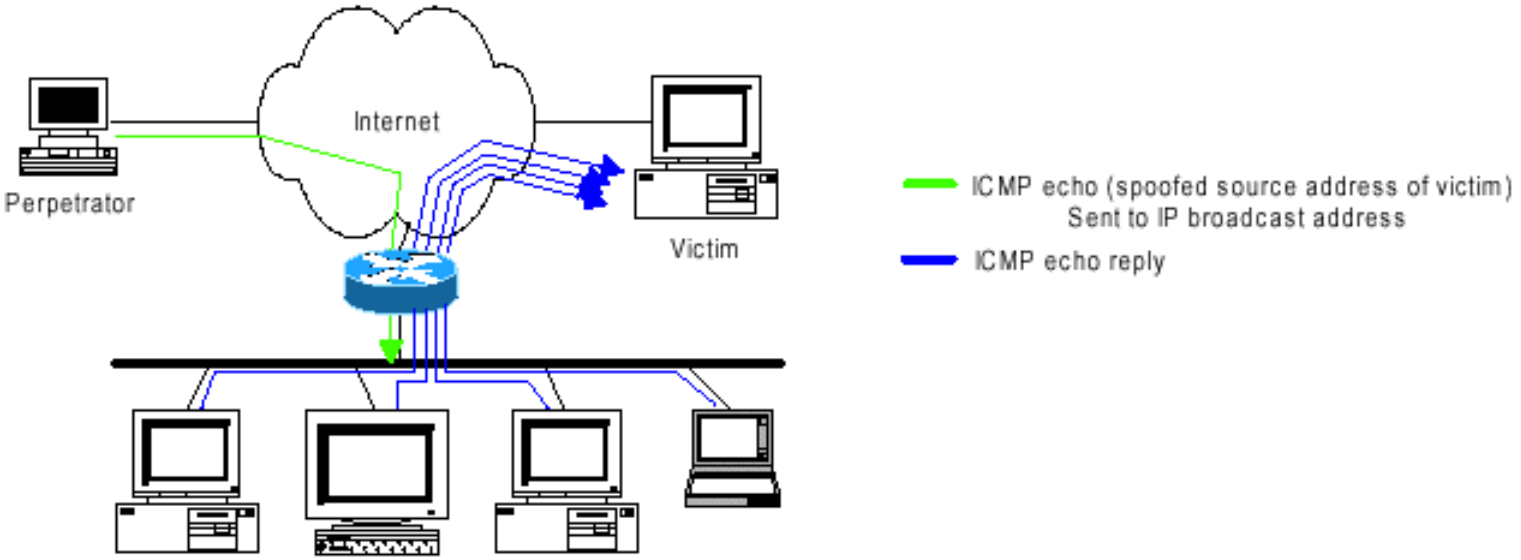
Integrità del routing – proxy arp

- Anche la funzionalità di proxy arp, attiva di default per permettere al router di rispondere per conto di altri hosts presenti sulla rete connessa può essere utilizzata allo scopo di perturbare l'integrità dell'instradamente. Pertanto è opportuno prevederne la disabilitazione a livello di interfacce esterne.

```
interface Serial0/1
    no ip proxy-arp
```

Denial of Service – Smurf/Fraggle

- **L'aggressore invia un grosso flusso di traffico ICMP echo verso una serie di indirizzi di broadcast attribuendosi come indirizzo sorgente quello della vittima. Se i router relativi alle reti di destinazione propagano i broadcast IP al livello 2 tutti gli hosts su tali reti risponderanno all'indirizzo falsificato con un echo-reply generando verso di esso un flusso di traffico pari a quello entrante moltiplicato per il loro numero**



Denial of Service – Smurf/Fraggle

- Il “fraggle” opera esattamente nella stessa maniera, usando però l’UDP echo invece di ICMP echo
- Entambi gli attacchi danneggiano fortemente sia la vittima che l’intermediario, o amplificatore
- Per evitare di fare da amplificatore è necessario disabilitare su tutti i router presenti sulla rete la propagazione dei broadcast a livello 2 su tutte le interfacce “broadcast enabled” (Ethernet, FDDI, FR/ATM in multipoint mode etc.)
- Il blocco dei broadcast è il default a partire dalla 12.0

```
interface Ethernet0
    no ip directed-broadast
```

Denial of Service – Ping Flooding

- Un altro comune DoS prevede il congestionamento di linee e il sovraccarico elaborativo di routers e hosts attraverso l'invio massivo e indiscriminato di ICMP ECHO request.
- La vittima di uno smurfing subisce un flooding
- L'uso del W*eighted Fair Queueing* si rivela piuttosto efficace per migliorare la tolleranza ai ping flooding

```
! Fair queueing with congestive discard treshold of 64 pkts
interface Serial 3/0
    ip unnumbered Ethernet 0/0
    fair-queue 64
```

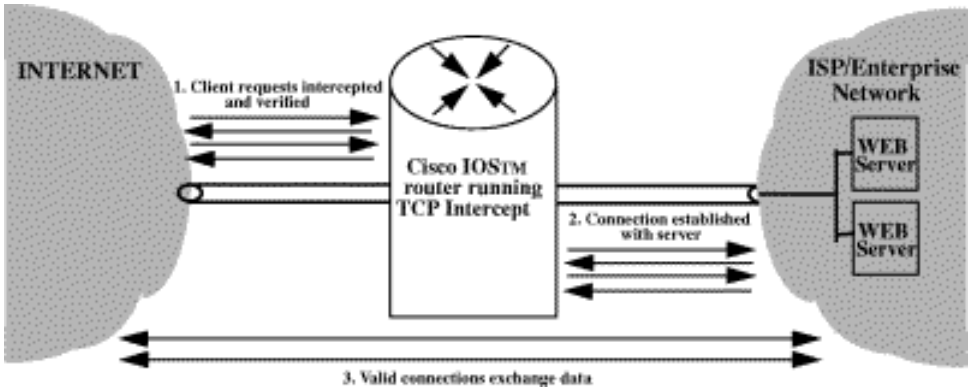
Denial of Service – SYN Flooding

- Il SYN flooding è una tecnica di DoS caratterizzata dall'apertura di un elevato numero di connessioni da indirizzi diversi, ovviamente falsificati, verso la vittima, curando di evitare l'*ACK* di chiusura del *TCP three way handshake* al fine di saturarne la coda di connessione
- E' possibile prevenire in maniera attiva tali attacchi attraverso l'abilitazione del *TCP intercept*

```
! Enable TCP intercept for selected net
ip tcp intercept list 101
access-list 101 permit tcp any 192.133.28.0 0.0.0.255
```

SYN flooding – TCP intercept

- Tale feature (IOS 11.2(4)F, 11.3 e successive) previene gli attacchi SYN-flood intercettando e validando (a la proxy) le richieste di connessione TCP verso gli hosts, definiti tramite un ACL, stabilendo una semiconnessione col client successivamente estesa al server in caso di successo



Ping Flooding - CAR

- E’ possibile reagire attivamente durante un attacco di tipo “ping flooding” per bloccare lo stesso o ridurne drasticamente l’impatto utilizzando il meccanismo di Committed Access Rate (CAR) previsto all’interno della funzionalità CEF per limitare in banda il flusso di traffico offensivo:

```
! ICMP echo traffic to limit
access-list 102 permit icmp any any echo
access-list 102 permit icmp any any echo-reply
interface Serial3/0/0
rate-limit input access-group 102 256000 8000 8000 conform-
    action transmit exceed-action drop
```

SYN Flooding - CAR

- Analogamente è possibile inibire i SYN flood verso particolari hosts senza influenzare le connessioni preesistenti:

```
! don't limit established TCP sessions non-SYN packets
access-list 103 deny tcp any host 10.0.0.1 established
! limit the rest of TCP (this really only includes SYNs)
access-list 103 permit tcp any host 10.0.0.1

interface Serial3/0/0
rate-limit input access-group 103 8000 8000 8000 conform-
    action transmit exceed-action drop
```

Flooding – Traffic Shaping

- Il Generic Traffic Shaping (GTS) è un meccanismo di packet filtering di tipo *token-bucket* che permette di imporre a un flusso di traffico IP un throughput massimo inferiore a quello nominale relativo all'interfaccia del router attraverso cui avviene la trasmissione. Tale meccanismo può essere utilizzato per prevenire DoS di tipo flooding predimensionando opportunamente la banda riservata al traffico sospetto

```
access-list 102 permit icmp any any
! Al traffico ICMP non piuo' essere garantito più di 1Mb
interface Serial0 traffic-shape group 101 1000000 125000
   125000
```

Denial of Service - Landing

- Il “land” o TCP loopback DoS è basato sull’invio di TCP SYN con indirizzo e porta sorgente falsificati e impostati identici a indirizzo e porta di destinazione. Questo può causare per release IOS meno recenti il blocco del router.
- Per prevenire il problema è necessario filtrare in ingresso su tutte le interfacce questo tipo di pacchetti:

```
access-list 111 deny ip host 143.225.190.25 host 143.225.190.25
access-list 111 deny ip host 142.225.98.254 host 142.225.98.254
access-list 111 permit ip any any
interface Serial 0/0
    ip access-group 111 in
interface Ethernet 1/0
    ip access-group 111 in
```

Denial of Service – Diag Ports

- L’invio di elevate quantità di traffico TCP o UDP sulle porte di diagnostica del router (*echo, discard, chargen, daytime*) può avere un notevole impatto sul carico elaborativo del router stesso, fino a degradarne fortemente le prestazioni o causarne, in condizioni estreme il blocco.
- E’ consigliabile quindi disabilitare (default a partire da IOS 12.0) tutti i servizi “diagnostic port”:

```
no service udp-small-servers
no service tcp-small-servers
```

Prevenzione DoS – Null last resort

- Una tecnica che spesso si rivela utile nel limitare i danni prodotti da DoS basati sull'invio di notevoli flussi di traffico è quella di prevedere staticamente come default gateway la null interface. Ciò comporta drastici miglioramenti in termini prestazionali nell'attività di scartare i pacchetti con indirizzo di destinazione non valido.

  ip route 0.0.0.0 0.0.0.0 null 0 255

- Naturalmente tale tecnica non è applicabile nei casi in cui la gestione del routing sia totalmente statica.

Prevenzione DoS – Scheduler

- Se sottoposto a grossi carichi di traffico, come nel caso di un attacco DoS, un router può trovarsi in una situazione di totale sovraccarico, dovuto alla necessità di gestire l'enorme quantità di interrupt generati dalle interfacce di rete e perciò in condizioni di non poter più attendere pienamente alle proprie attività. Si può migliorare la situazione costringendo il router a fermarsi a intervalli regolari nell'attività di gestione degli interrupt per dedicarsi ad assolvere ai rimanenti tasks a livello di processi.

```
scheduler interval 500
! In later version substituted by allocate option
scheduler allocate 250000 10000
```

Prevenzione DoS - SPD

- Una tecnica utilizzata per limitare il danno relativo alla mancata propagazione delle informazioni di routing su collegamenti in congestione a seguito di atacchi DoS è l’abilitazione della funzionalità di Selective Packet Discard (SPD). Nel meccanismo di scarto di pacchetti su interfacce relative a link a elevato livello di saturazione, tale feature favorisce la perdita selettiva di pacchetti possibilmente non relativi a informazioni di routing dinamico

```
ip spd enable
```

Prevenzione DoS - Nagle

- L’abilitazione dell’algoritmo di Nagle per il controllo della congestione è estremamente utile per facilitare l’accesso remoto via telnet al router da parte degli amministratori anche in situazioni di grave congestione del canale di accesso allo stesso
- Scopo dell’algoritmo è evitare la proliferazione di pacchetti di piccole dimensioni raccogliendo i caratteri delle sessioni in blocchi e trasmettendoli a intervalli regolari (in corrispondenza degli ACK)

service nagle

Prevenzione - Servizi innecessari

- E’ certamente opportuno disabilitare tutti i servizi non strettamente necessari che il router fornisce di default e che potrebbero presentare eventuali debolezze o fornire informazioni riservate all’esterno circa i dettagli della rete interna

```
no service finger
no service pad
no ip bootp server
! Cisco discovery protocol (info su router connessi)
no cdp run
```

Logging

- E’ buona regola, alla base di ogni politica di sicurezza, salvare (syslogd) e conservare informazioni dettagliate di logging relative a tutti gli eventi segnalati dal sistema, fra cui accessi, riconfigurazioni e informazioni di servizio, su un host opportunamente configurato:

```
service timestamps debug datetime localtime show-timezone msec
service timestamps log datetime localtime show-timezone msec
logging buffered 16384
logging trap debugging
logging facility local7
logging 192.133.28.3
logging source-interface Serial 0
```

Auditing

- Analogamente e’ possibile effettuare un accounting completo degli accessi e dei comandi su host remoto utilizzando radius o tacacs+

```
aaa new-model
aaa authentication login default tacacs+ enable
aaa authentication enable default tacacs+ enable
aaa accounting command 15 start-stop tacacs+
aaa accounting exec start-stop tacacs+
ip tacacs source-interface Loopback0
tacacs-server host 192.132.34.41
tacacs-server key MyKey
```