



Implementing Secure Converged Wide Area Networks (ISCW)

Cisco IOS Firewall

<http://www.INE.com>

Firewall Design Overview

- Firewall defines traffic interaction between “zones” or trust levels
 - e.g. ASA `security-level`
- Common zone definitions
 - Inside
 - Most trusted network
 - Outside
 - Least trusted network
 - DMZ
 - Somewhere in between

Copyright © 2009 InternetNetwork Expert, Inc
www.INE.com



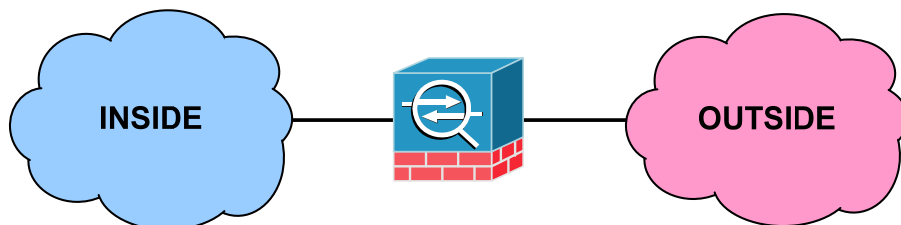
Firewall Filtering Logic

- Allow traffic from trusted zones to untrusted zones
 - Return traffic should be okay
- Block traffic from untrusted zones to trusted zones

Copyright © 2009 Internetwork Expert, Inc
www.INE.com

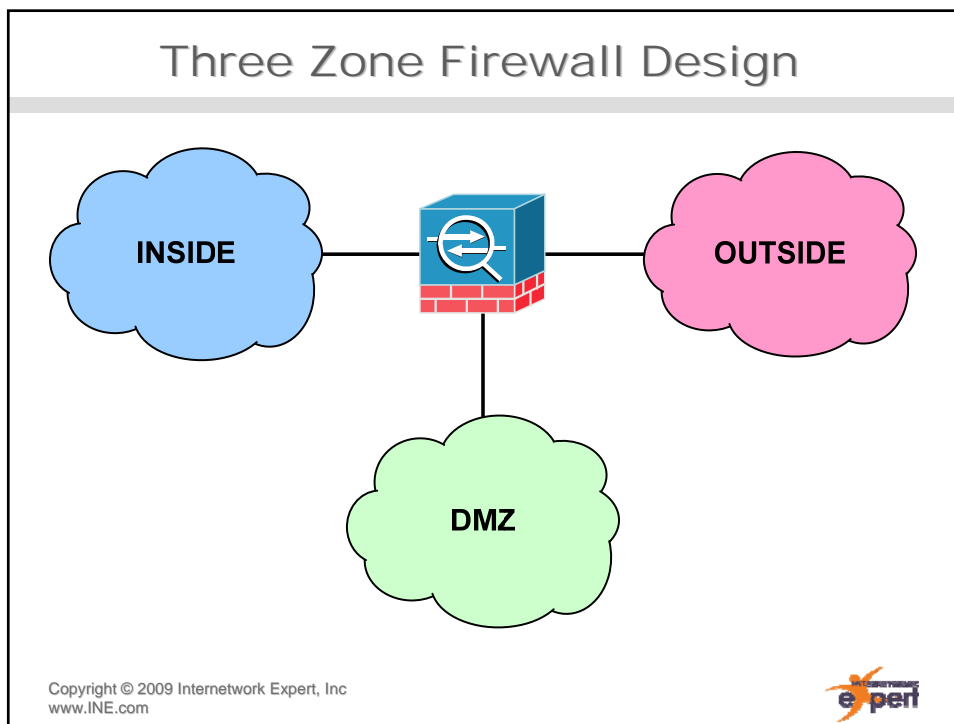



Two Zone Firewall Design



Copyright © 2009 Internetwork Expert, Inc
www.INE.com





- ### Three Zone Firewall Problems
- Which is the “more” trusted zone?
 - Typical logic is...
 - Inside to outside allowed
 - Return traffic okay
 - Inside to DMZ allowed
 - Return traffic okay
 - Outside to DMZ allowed
 - Return traffic okay
 - DMZ to inside/outside dropped
 - Why would DMZ originate traffic?
- Copyright © 2009 Internetwork Expert, Inc
www.INE.com
- 

Types of Firewalls

- Stateless packet filters
- Application Level Gateways (ALG)
- Stateful packet filter

Copyright © 2009 Internetwork Expert, Inc
www.INE.com



Stateless Packet Filters

- Statically configured filters
 - e.g. extended ACLs
- Typically filter based on...
 - Layer 3
 - Source & destination address
 - Protocol number
 - Layer 4
 - Source & destination port
 - Established flags
- Problems
 - Management overhead
 - Complex design not feasible
 - e.g. three or more zones

Copyright © 2009 Internetwork Expert, Inc
www.INE.com



Application Level Gateways

- AKA Proxy Servers
 - Client connects to proxy
 - Proxy connects to destination on behalf of client
- Advantage
 - Adds application level awareness to filtering
- Disadvantage
 - Typically PPS limitations

Copyright © 2009 Internetwork Expert, Inc
www.INE.com



Stateful Firewalls

- Dynamic filtering based on session tracking
 - What goes out must come back in
- “State” of flow typically tracked by
 - Source & destination address
 - Source & destination port
 - Protocol flags
 - e.g. SYN, ACK/SYN, FIN, RST

Copyright © 2009 Internetwork Expert, Inc
www.INE.com



Stateful Firewall Problems

- Not all protocols “stateful”
 - UDP is connectionless
- Non-standard applications
 - Outbound and inbound flows not mirror images
 - e.g. HTTP (standard) vs. FTP (non-standard)

Copyright © 2009 Internetwork Expert, Inc
www.INE.com



IOS Firewall Feature Set

- IOS Firewall
- Authentication Proxy
- IOS Intrusion Prevention System (IPS)

Copyright © 2009 Internetwork Expert, Inc
www.INE.com



IOS Firewall

- Combination of multiple features to obtain ALG based stateful firewall
- Previously...
 - CBAC & `ip inspect`
 - Reflexive ACLs before that
- Currently...
 - Zone Based Policy Firewall (ZBPF)
- Adds ALG support to state tracking
 - e.g. I know FTP is different inbound vs. outbound
- Includes SYN flood protection
 - Previously TCP Intercept

Copyright © 2009 Internetwork Expert, Inc
www.INE.com



Authentication Proxy

- Tracks inside to outside traffic flows
- Denied flows can trigger authentication request towards AAA
- If authentication successful, per-user ACL is downloaded from AAA
 - Both TACACS+ and RADIUS support
- Scalable solution for what used to be “Lock-and-Key”
 - AKA “dynamic” ACL

Copyright © 2009 Internetwork Expert, Inc
www.INE.com



IOS IPS

- Tracks traffic flows against “signature” database
- Takes action based on matches
 - e.g. alarm, drop, reset, etc.
- More detail later...

Copyright © 2009 Internetwork Expert, Inc
www.INE.com



Configuring Stateless Filters

- Standard ACLs
 - Match only on source IP address
- Extended ACLs
 - Match on...
 - IP protocol number
 - Source address
 - Destination address
 - Protocol options
 - TCP / UDP ports (eq, neq, lt, gt, range)
 - ICMP Type Code
 - Packet markings
 - DSCP
 - IP Precedence
 - TOS
- ACL logging support

Copyright © 2009 Internetwork Expert, Inc
www.INE.com



Configuring CBAC

- Define inspection rule
- Define untrusted to trusted stateless filter
 - CBAC exceptions
 - Implicit/explicit deny
- Apply inspection rule
 - Inside in
 - Outside out
- Optional
 - Audit rules
 - SYN flood protection
- Verification and monitoring
 - `show ip inspect sessions`

Copyright © 2009 Internetwork Expert, Inc
www.INE.com



Basic CBAC Configuration

```
R6#
ip inspect name CBAC tcp
ip inspect name CBAC udp
ip inspect name CBAC icmp
!
ip access-list extended OUTSIDE_IN
deny ip any any
!
interface FastEthernet0/1
ip access-group OUTSIDE_IN in
ip inspect CBAC out
```

Copyright © 2009 Internetwork Expert, Inc
www.INE.com



Zone Based Policy Firewall

- Uses ASA logic of application specific class-maps & policy-maps to match traffic and...
 - Inspect
 - Drop
 - Pass
- Allows complex designs to be more modular
 - e.g. multiple DMZs
- Much more granular support for application inspection
- Configuration more cumbersome, but workflow more logical
 - e.g. basic SDM config is 50+ lines

Copyright © 2009 Internetwork Expert, Inc
www.INE.com



Basic ZBPF Configuration

```
R6#
class-map type inspect match-any INSPECTIONS
  match protocol tcp
  match protocol udp
  match protocol icmp
!
policy-map type inspect INSIDE_TO_OUTSIDE
  class type inspect INSPECTIONS
    inspect
  class class-default
    drop
!
zone security INSIDE
zone security OUTSIDE
zone-pair security INSIDE_TO_OUTSIDE source INSIDE destination OUTSIDE
  service-policy type inspect INSIDE_TO_OUTSIDE
!
interface FastEthernet0/0
  zone-member security INSIDE
!
interface FastEthernet0/1
  zone-member security OUTSIDE
```

Copyright © 2009 Internetwork Expert, Inc
www.INE.com



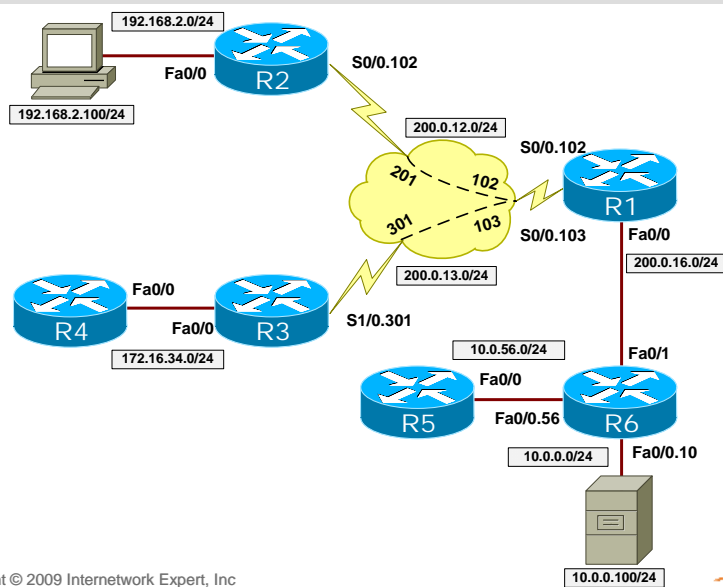
ZBPF Verification

- What are the zones?
 - `show zone security`
- Where are they applied?
 - `show zone-pair security`
- What is being inspected?
 - `show class-map type inspect`
- How is it being inspected?
 - `show policy-map type inspect`
- What are the overall statistics?
 - `show policy-map type inspect zone-pair`
- What are the current sessions?
 - `show policy-map type inspect zone-pair sessions`

Copyright © 2009 Internetwork Expert, Inc
www.INE.com



IOS Firewall Configuration Examples



Copyright © 2009 Internetwork Expert, Inc
www.INE.com

