

# Discussion of Conceptual Difference Between Cisco IOS Classic and Zone-Based Firewalls

## Introduction

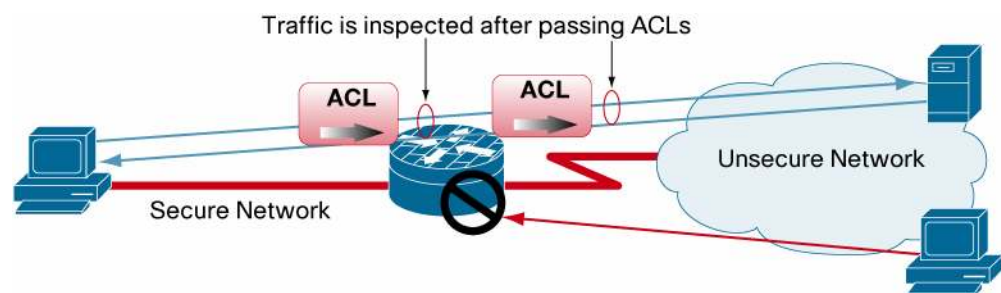
Cisco IOS has supported stateful inspection firewall capability since before Cisco IOS Software Version 12.0. Stateful Inspection Firewall features are supported through the Classic Firewall (formerly known as Context-Based Access Control, or CBAC). Cisco IOS Software introduced an additional configuration model for stateful inspection with the Zone-Based Policy Firewall (ZFW) in Cisco IOS Software version 12.4(6)T. Cisco IOS Software Classic Firewall will continue to be maintained for the foreseeable future, but will not be significantly enhanced with new features. Instead, the strategic development direction for Cisco IOS Software's stateful inspection firewall is carried by Zone-Based Policy firewall.

## Policy Differences Between Classic Firewall and Zone-Based Policy

Classic Firewall and Zone-Based Policy Firewall differ substantially in their policy configuration concepts.

Classic Firewall policy is defined by applying static Access-Control List (ACL) configuration on router interfaces to define the types of traffic allowed through an interface. Stateful Packet Inspection is applied with "ip inspect" policies that monitor network traffic to allow desired return traffic through ACLs that would otherwise drop traffic that had been originated by trusted hosts. Complex Classic Firewall policy extrapolation may be difficult in circumstances where multiple ACLs affect traffic, especially when ACLs were applied for both router-local traffic as well as traffic "transiting" (entering the router and leaving by the same or a different interface) the router.

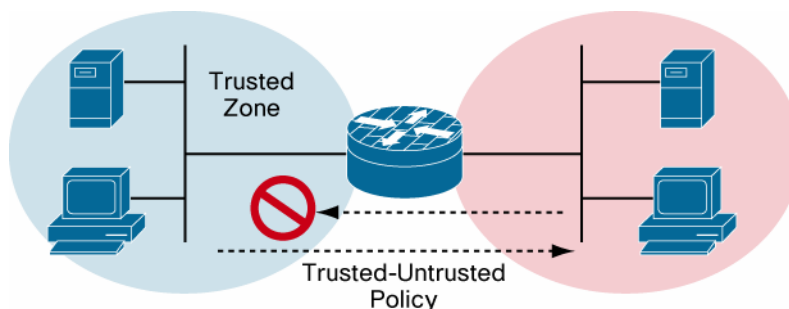
Figure 1.



Zone-Based Policy Firewall changes the IOS Stateful Inspection model from Classic Firewall's 'interface-based' model to a more flexible, easier-understood zone-based configuration model. Router interfaces are assigned to security zones, and firewall inspection policy is applied to traffic moving between the zones. Zone-Based Policy Firewall enforces a secure inter-zone policy by default, such that a given interface cannot pass traffic to interfaces in other security zones until an explicit policy allowing traffic is defined. Firewall policies are configured using Class-Based Policy Language (CPL), which employs a hierarchical structure to define inspection for network protocols and the groups of hosts' traffic to which inspection will be applied. Inter-zone policies offer

considerable flexibility and granularity, so different inspection policies can be applied to hosts, host groups, or subnets connected to the same router interface.

**Figure 2.**



Each interface can be a member of only one security zone, but zones can hold multiple interfaces. When an interface is made a zone-member, traffic will not pass between a given interface and interfaces in other zones until an explicit policy is configured to allow desired traffic. Zone-Based Policy Firewall enforces a default policy blocking traffic between zones.

Policies are established by configuring a class to define the traffic that the policy affects, then defining a policy that associates the traffic class with a given action, such as inspect, pass, or drop. Additional parameters can be applied to specify connection volumes or actions such as URL filtering for HTTP traffic. Policy-maps are associated with zone pairs to apply unidirectional traffic policy to traffic moving from one zone to another.

For more detailed discussion of Zone-Based Policy Firewall Concepts and Applications, refer to the Zone-Based Firewall Design Guide and Zone-Based Policy Firewall Configuration Guide indicated in the “Additional Reading” portion of this document.

## Feature Parity

Cisco IOS Classic Firewall has been substantially enhanced during its lifetime. Zone-Based Policy Firewall addresses most of the functionality offered by the Classic Firewall, and is beginning to draw clear differentiators to address needed capabilities. Refer to Table 1 for a feature comparison between Cisco IOS Classic and Zone-Based Policy Firewall:

**Table 1.** Feature parity comparison between Cisco IOS Classic and Zone-Based Policy Firewall

Feature	Classic Firewall Support	Zone Firewall Support
<b>Stateful Inspection</b>	Yes—Pre-12.0	Yes—12.4(6)T
<b>Instant Messaging Application Inspection and Control</b>	Yes—12.4(2)T	Yes—12.4(9)T
<b>Virtual (VRF-Aware) Firewall</b>	Yes—12.4(4)T	Yes—12.4(6)T
<b>HTTP Application Inspection and Control</b>	Yes—12.4(4)T	Yes—12.4(9)T
<b>Heuristics-Based Peer-to-Peer Application Inspection and Control</b>	No	Yes—12.4(9)T
<b>IPv6 Stateful Inspection</b>	Yes—12.3(7)T	No*
<b>Unified Firewall SNMP MIB</b>	Yes—12.4(6)T	No*
<b>Active-Standby Stateful Failover</b>	Yes—12.4(6)T	No*
<b>Advanced Voice Service Inspection</b>	No	First Half CY08
<b>User-Based Policy Firewall Inspection</b>	Yes (Auth-Proxy)—12.2(8)T	First Half CY08

\* These capabilities are being investigated for inclusion in a future software release

## Router Platform and Management Support

Classic Firewall is supported throughout the Cisco IOS router product family. Zone-Based Policy firewall support is limited to platforms that include the Cisco IOS Quality of Service system. Supported platforms are described in Table 2:

**Table 2.** Router platform support for Cisco IOS Classic and Zone-Based Policy Firewall

Router Platform	Classic Firewall Support	Zone-Based Policy Firewall Support
850 Series	Yes	No
870 Series	Yes	Yes
1701,1711,1712,1721,1751	Yes	Yes
1800 Series	Yes	Yes
2600XM Series, 2691	Yes	Yes
2800 Series	Yes	Yes
3700 Series	Yes	Yes
3800 Series	Yes	Yes
7200 Series	Yes	Yes
7301	Yes	Yes
7400 Series	Yes	No
UC500 Series	Yes	Yes

Graphical User Interface management for both firewalls is offered by Cisco Security Device Manager (SDM). Cisco Security Manager (CSM) only supports the Cisco IOS Classic Firewall at present, but future support for Zone-Based Policy Firewall in CSM is planned.

## Conclusion

Cisco IOS Software Release 12.4(6)T introduced dramatic changes to default security posture and configuration model with Cisco IOS Zone-Based Policy Firewall. New features will only be introduced in the Zone-Based Policy Firewall. To take advantage of new capabilities, existing Classic IOS Firewall configurations will need to be migrated to Zone-Based Policy Firewall configuration.

## Additional Reading

Zone-Based Policy Firewall Design and Application Guide

[http://www.cisco.com/en/US/products/sw/secursw/ps1018/products\\_configuration\\_example09186a00808bc994.shtml](http://www.cisco.com/en/US/products/sw/secursw/ps1018/products_configuration_example09186a00808bc994.shtml).



**Americas Headquarters**  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
www.cisco.com  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 527-0883

**Asia Pacific Headquarters**  
Cisco Systems (USA) Pte. Ltd.  
168 Robinson Road  
#28-01 Capital Tower  
Singapore 068912  
www.cisco.com  
Tel: +65 6317 7777  
Fax: +65 6317 7799

**Europe Headquarters**  
Cisco Systems International BV  
Haarlerbergpark  
Haarlerbergweg 13-19  
1101 CH Amsterdam  
The Netherlands  
www-europe.cisco.com  
Tel: +31 0 800 020 0791  
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

©2007 Cisco Systems, Inc. All rights reserved. CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDR, CCIE, CCIP, CCNA, CCNP, CCSR, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0710R)