Access Control Policy – Firewalls

Access policy rules provide access control because they define which packets are permitted and which are denied. A firewall access policy consists of a set of rules. Each packet is analyzed and its elements compared against elements in the rules of the policy sequentially, from top to bottom. The first rule that matches the packet has its configured action applied, and any processing specified in the rule's configured options is performed.

Each rule has a standard set of rule elements against which packet characteristics are compared. These rule elements, displayed as fields in the rule, include the packet's source address (Source), its destination address (Destination), its protocol and port numbers (Service), the interface it is passing through (Interface), its direction of travel (Direction), and the time of its arrival (Time). For example, if a packet entering the firewall has a source address that matches the object in the Source field of the rule, its destination address matches the object in the Destination field, its protocol and port numbers match the object in the Service field, the interface it passes through matches the interface object in the Interface field, its direction matches that specified in the Direction field, and the time of its arrival matches that specified in the Time field, then the firewall takes the actions specified in the Action field and applies the options specified in the Options field. A field where a value of "Any" or "All" is specified is considered to match all packets for that rule element.

For example, in Figure 1, rule #0 is "anti-spoofing": it denies all packets coming through the outside interface with source address claiming to be that of the firewall itself or internal network it protects. This rule utilizes interface and direction matching in addition to the source address. Rule #2 says that connection from the internal network (network object **net-192.168.1.0**) to the firewall itself (object **firewall**) using **ssh** is allowed (action **Accept**). The "Catch all" rule #6 denies all packets that have not been matched by any rule above it. The access policy in Figure 1 is constructed to allow only specific services and deny everything else, which is a good practice.

		Source	Destination	Service	Interface	Direction	Action	Comment
0		firewall net-192.168.1.0	Any	Any	outside	Inbound	Deny	anti spoofing rule
1		Any	Any	Any	loopback	Both	Accept	
2		net-192.168.1.0	firewall	ssh	All	Both	Accept	SSH Access to firewall is permitted
3		firewall	net-192.168.1.0	DNS	All	Both	Accept	Firewall uses one of the machines
4		Any	firewall	Any	All	Both	Deny	All other attempts to connect to
5		net-192.168.1.0	Any	Any	All	Both	Accept	
6		Any	Any	Any	All	Both	Deny	

Figure 1 Access policy rules

By default, a rule matches on specified Source, Destination, and Service rule elements, matching all interfaces and traffic directions. If you want to restrict the effect of the rule to particular interfaces or traffic directions, you must specify the restriction in the rule.