

Firewall Policy Comparison Report

Source host:acmecorp-pix

config.txt : C:\Documents and Settings\hurst\Desktop\firewall configs\acme-pix\config.txt
 route.txt : C:\Documents and Settings\hurst\Desktop\firewall configs\acme-pix\route.txt

Target host:acmecorp-pix

config.txt : C:\Documents and Settings\hurst\Desktop\firewall configs\acme-pix\config-diff-obj.txt
 route.txt : C:\Documents and Settings\hurst\Desktop\firewall configs\acme-pix\route.txt

Completed on Thu Jul 15 11:45:18 CDT 2010

The policy comparison diff reports lists all the policy differences found between the two firewalls in a tabular format described below. Policy diffs may be performed between configurations of the same firewall in the context of change modeling and verification, or during a migration involving a source and target firewalls of different types, such as Cisco Devices to Check Point.

Policies are compared taking into account acl, NAT, and routing rules in both firewalls. In a migration context, the route rules for the target firewall configuration may not be available, and hence the routing rules of the source configuration are used in the target configuration as well, for policy comparisons.

Policy diffs for migration assumes that the migration is being done "in place", meaning that locally connected and reachable networks remain unchanged. These mappings are determined using network reachability, calculated from the routing tables of both firewalls. In many cases, these mappings are one-to-one, but there can be situations where interfaces in one firewall are dropped, split, or combined in the other. Ipsec interfaces are mapped separately, but in the same way by comparing reachable networks. Management interfaces are not mapped.

In the following report "Left" and "Right" refer to "acmecorp-pix".

Reachability Table for Left firewall

Zone	Interface	Reachable Networks
DMZ	mail1 (192.168.1.1/255.255.255.0)	192.168.1.0/24
	proxymail (192.168.9.1/255.255.255.0)	192.168.9.0/24
	testweb (192.168.50.1/255.255.255.0)	192.168.50.0/24
External	outside (62.59.14.189/255.255.255.224)	0.0.0.0 to 9.255.255.255 11.0.0.0 to 172.15.255.255 172.18.0.0 to 192.168.0.255 192.168.6.0 to 192.168.8.255
		192.168.10.0 to 192.168.49.255 192.168.51.0 to 255.255.255.255

Zone	Interface	Reachable Networks
Internal	inside (172.16.0.1/255.255.0.0)	10.0.0.0/8 172.16.0.0/15 192.168.2.0 to 192.168.5.255

Reachability Table for Right firewall

Zone	Interface	Reachable Networks
DMZ	mail1 (192.168.1.1/255.255.255.0)	192.168.1.0/24
	proxymail (192.168.9.1/255.255.255.0)	192.168.9.0/24
	testweb (192.168.50.1/255.255.255.0)	192.168.50.0/24
External	outside (62.59.14.189/255.255.255.224)	0.0.0.0 to 9.255.255.255 11.0.0.0 to 172.15.255.255 172.18.0.0 to 192.168.0.255 192.168.6.0 to 192.168.8.255
		192.168.10.0 to 192.168.49.255 192.168.51.0 to 255.255.255.255
Internal	inside (172.16.0.1/255.255.0.0)	10.0.0.0/8 172.16.0.0/15 192.168.2.0 to 192.168.5.255

Interface Map

Left Interface	IP Address	Right Interface	IP Address
inside	172.16.0.1/255.255.0.0	inside	172.16.0.1/255.255.0.0
mail1	192.168.1.1/255.255.255.0	mail1	192.168.1.1/255.255.255.0
outside	62.59.14.189/255.255.255.224	outside	62.59.14.189/255.255.255.224
proxymail	192.168.9.1/255.255.255.0	proxymail	192.168.9.1/255.255.255.0
testweb	192.168.50.1/255.255.255.0	testweb	192.168.50.1/255.255.255.0

In the following policy diff table, we follow the convention of showing each policy diff item that is added (or deleted) from the right firewall. A hyperlink can be traversed to view the Policy Diff Rule Trails report that describes the configuration rule (acl, NAT, and Route) numbers involved in that policy in both firewalls. The actual rules (or their vendor view in the case of Check Point firewalls) can be viewed in the configuration report by traversing respective hyperlinks.

Services Passing Through Firewall

This section lists source and destination addresses for all IP services that are allowed to pass through the firewall device. The list of allowed services is grouped by each output interface from which the allowed IP traffic leaves the firewall.

Entering/Exiting Interface	Service	Src Address	Dst Address	Comment
proxymail -> Right:acmecorp-pix ->	tcp/imap4 (143)	192.168.9.2	0.0.0.0 to 9.255.255.255	Added Policy
			11.0.0.0 to 172.15.255.255	Added Policy
			172.18.0.0 to 192.168.0.255	Added Policy
			192.168.6.0 to 192.168.8.255	Added Policy
			192.168.10.0 to 192.168.49.255	Added Policy
			192.168.51.0 to 255.255.255.255	Added Policy