NETWORK INTELLIGENCE
An ISO 27001 Company

Firewall Analysis Report

Report Date
11/18/2015 3:09:12 PM

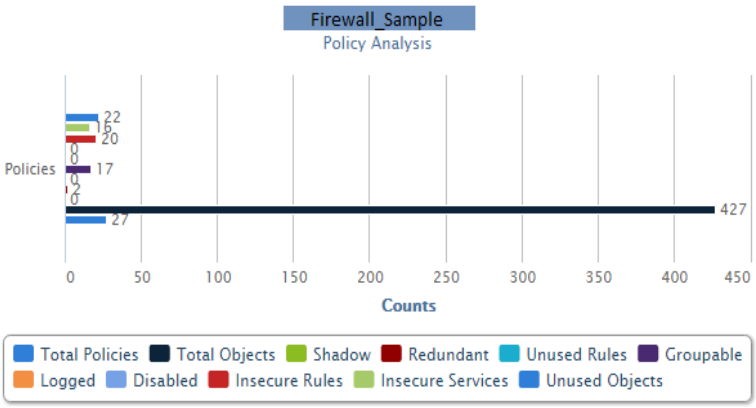
Table of Contents

Firewall Details

Network	Firewall	Hostname	Domain Name	Type	Added On
Juniper	FirewallSample	SampleHost		Junos	9/12/2014 3:04:10 PM

Statistics

Category	Total Policies	Total Objects	Redundant	Unused Rules	Shadow	Groupable	Logged	Disabled	Insecure Access Rule	Insecure Services	Unused Objects
Count	18	50	0	0	0	8	0	0	7	18	3
%	-	-	0%	0%	0%	44%	0%	0%	38%	100%	6%



Shadow Rules

These rules are often implemented to handle some emergency or critical worm infection. They are found to be completely in contradiction to an already existing rule. The end-result depends on the sequence of the 2 rules. Some firewalls (Netscreen mostly) warn you if you're creating a rule in contradiction to an existing rule.

Below is a list of shadow rules in which rules are same having opposite actions.

#	Line	Policy ID	From Zone	To Zone	Source	Destination	Service	Action	Status	Justification
Total 0 items.										

Redundant Rules

Often once a request has passed through all the change management steps, it comes to the firewall administrator, who upon seeing all the t's are crossed and i's are dotted, simply goes and implements the rule on to the firewall configuration. Rarely if ever does he check if the rule might already be in existence or he may have created a super set of an existing rule, thus making the earlier one redundant.

Below is a list of redundant rules in which rules might be similar or subset of the first rule.

#	Line	Policy ID	From Zone	To Zone	Source	Destination	Service	Action	Status	Justification
Total 0 items.										

Unused Rules

As networks are dynamic, systems come and go. But firewall rules tend to remain forever.Child rules are the rules defined after the parent rule.Child rules are either subset or similar to the parent rule, so the child rules are never hit.

Below is a list of unused rules in which rules are defined but never hit.

#	Line	Policy ID	From Zone	To Zone	Source	Destination	Service	Action	Status	Justification
Total 0 items.										

Insecure Access Rules

Below is a list of insecure access rules in which rules are defined on the basis of either source or destination address having any, ftp or telnet.

#	Line	Policy ID	From Zone	To Zone	Source	Destination	Service	Action	Status	Justification
1	203	P53	Fzone1	Tzone1	Source1	Source2	any	Permit	Active	
2	223	P50	Fzone1	Tzone1	Source1	Source3	any	Permit	Active	
3	247	P4	Tzone1	Fzone1	Source2	Source1	any	Permit	Active	
4	266	P1	Tzone1	Fzone1	Source3	Source1	any	Permit	Active	
5	270	P100	Source4	Fzone1	Source4	Source1	junos-ftp junos-icmp-all junos-ntp junos-ping junos-ssh junos-tftp	Permit	Active	
6	279	P151	Fzone1	Source4	Source1	Source4	junos-ftp junos-icmp-all junos-ntp junos-ping junos-ssh junos-tftp	Permit	Active	
7	288	P57	Fzone1	Fzone1	any	any	any	Permit	Active	
Total 7 items.										

Large Subnets

Below is a list of large subnets in which rules are defined on the basis of IP address which contains subnets less than or equal to 24.

#	Line	Zone	Address	IP Address	Group
1	298	Tzone1	Address1	1.1.1.0/24	Source2
2	305	Tzone1	Address2	1.1.1.0/23	Source3
3	306	Tzone1	Address3	1.1.1.0/17	Source3
4	367	Source4	Address6	1.1.1.0/17	Source4
5	368	Source4	Address4	1.1.1.0/17	Source4
Total 5 items.					

Critical Ports

Below is a list of critical ports in which rules are defined on the basis of service containing either any, ftp, telnet, vnc, oracle, sql.

#	Line	Policy ID	From Zone	To Zone	Source	Destination	Service	Action	Status	Justification
1	187	P56	Fzone1	Tzone1	Source1	Source5	junos-ftp junos-icmp-all junos-ssh	Permit	Active	

							junos-telnet junos-tftp			
2	195	P55	Fzone1	Tzone1	Source1	Dest1	any	Permit	Active	
3	199	P54	Fzone1	Tzone1	Source1	Source7	any	Permit	Active	
4	203	P53	Fzone1	Tzone1	Source1	Source2	any	Permit	Active	
5	207	P52	Fzone1	Tzone1	Source1	Dest3	junos-ftp junos-icmp-all junos-ntp junos-tftp	Permit	Active	Active
6	214	P51	Fzone1	Tzone1	Source1	Dest4	junos-ftp junos-icmp-all junos-ntp junos-ssh junos-telnet junos-tftp	Permit	Active	
7	223	P50	Fzone1	Tzone1	Source1	Source3	any	Permit	Active	
8	227	Sample	Fzone1	Tzone1	Source6	Dest5 Dest6	any	Permit	Active	
9	232	P7	Tzone1	Fzone1	Source5	Source1	junos-ftp junos-icmp-all junos-ssh junos-tftp	Permit	Active	
10	239	P6	Tzone1	Fzone1	Dest1	Source1	any	Permit	Active	
11	243	P5	Tzone1	Fzone1	Source7	Source1	any	Permit	Active	
12	247	P4	Tzone1	Fzone1	Source2	Source1	any	Permit	Active	
13	251	P3	Tzone1	Fzone1	Dest3	Source1	junos-ftp junos-icmp-all junos-ntp junos-ssh	Permit	Active	
14	258	P2	Tzone1	Fzone1	Dest4	Source1	junos-ftp junos-icmp-all junos-ntp junos-ssh junos-telnet	Permit	Active	
15	266	P1	Tzone1	Fzone1	Source3	Source1	any	Permit	Active	
16	270	P100	Source4	Fzone1	Source4	Source1	junos-ftp junos-icmp-all junos-ntp junos-ping junos-ssh junos-tftp	Permit	Active	
17	279	P151	Fzone1	Source4	Source1	Source4	junos-ftp junos-icmp-all junos-ntp junos-ping junos-ssh junos-	Permit	Active	

							tftp			
18	288	P57	Fzone1	Fzone1	any	any	any	Permit	Active	
Total 18 items.										

Service Grouping

Below is a list of service grouping in which rules are grouped on the basis of same source and destination having different service.

#	Line	Policy ID	From Zone	To Zone	Source	Destination	Service	Action	Status	Justification
Total 0 items.										

Destination Grouping

Below is a list of destination grouping in which rules are grouped on the basis of same source and service having different destination.

#	Line	Policy ID	From Zone	To Zone	Source	Destination	Service	Action	Status	Justification
1	195	P55	Fzone1	Tzone1	Source1	Dest1	any	Permit	Active	
	199	P54	Fzone1	Tzone1	Source1	Source7	any	Permit	Active	
	203	P53	Fzone1	Tzone1	Source1	Source2	any	Permit	Active	
	223	P50	Fzone1	Tzone1	Source1	Source3	any	Permit	Active	
Total 1 items.										

Source Grouping

Below is a list of source grouping in which rules are grouped on the basis of same destination and service having different source.

#	Line	Policy ID	From Zone	To Zone	Source	Destination	Service	Action	Status	Justification
1	239	P6	Tzone1	Fzone1	Dest1	Source1	any	Permit	Active	
	243	P5	Tzone1	Fzone1	Source7	Source1	any	Permit	Active	
	247	P4	Tzone1	Fzone1	Source2	Source1	any	Permit	Active	
	266	P1	Tzone1	Fzone1	Source3	Source1	any	Permit	Active	
Total 1 items.										

Unused Address

Below is a list of unused address in which addresses are defined but never used.

#	Line	Name	Type	IP Address	Zone
1	314	Sample_unused1	Host	1.1.1.1	Tzone1
Total 1 items.					

Unused Address Set

Below is a list of unused address set in which group of addresses are defined but never used.

#	Line	Name	Zone
1	338	UnusedAddress1	Tzone1
2	332	UnusedAddress2	Tzone1
Total 2 items.			

Unused Application

Below is a list of unused application in which services are defined but never used.

#	Line	Name	Term	Protocol	Source Port	Destination Port
No items available to display.						

Unused Application Set

Below is a list of unused application set in which group of services are defined but never used.

#	Line	Name
No items available to display.		

All Policies

Below is a list of all policies.

#	Line	Policy ID	From Zone	To Zone	Source	Destination	Service	Action	Status	Logged	Justification
1	187	P56	Fzone1	Tzone1	Source1	Source5	junos-ftp junos-icmp-all junos-ssh junos-telnet junos-tftp	Permit	Active	False	
2	195	P55	Fzone1	Tzone1	Source1	Dest1	any	Permit	Active	False	
3	199	P54	Fzone1	Tzone1	Source1	Source7	any	Permit	Active	False	
4	203	P53	Fzone1	Tzone1	Source1	Source2	any	Permit	Active	False	
5	207	P52	Fzone1	Tzone1	Source1	Dest3	junos-ftp junos-icmp-all junos-ntp junos-tftp	Permit	Active	False	
6	214	P51	Fzone1	Tzone1	Source1	Dest4	junos-ftp junos-icmp-all junos-ntp junos-ssh junos-telnet junos-tftp	Permit	Active	False	
7	223	P50	Fzone1	Tzone1	Source1	Source3	any	Permit	Active	False	
8	227	Sample	Fzone1	Tzone1	Source6	Dest5 Dest6	any	Permit	Active	False	
9	232	P7	Tzone1	Fzone1	Source5	Source1	junos-ftp junos-icmp-all junos-ssh junos-tftp	Permit	Active	False	
10	239	P6	Tzone1	Fzone1	Dest1	Source1	any	Permit	Active	False	
11	243	P5	Tzone1	Fzone1	Source7	Source1	any	Permit	Active	False	
12	247	P4	Tzone1	Fzone1	Source2	Source1	any	Permit	Active	False	
13	251	P3	Tzone1	Fzone1	Dest3	Source1	junos-ftp junos-icmp-all junos-ntp junos-ssh	Permit	Active	False	
14	258	P2	Tzone1	Fzone1	Dest4	Source1	junos-ftp junos-icmp-all junos-ntp junos-ssh junos-telnet	Permit	Active	False	
15	266	P1	Tzone1	Fzone1	Source3	Source1	any	Permit	Active	False	
16	270	P100	Source4	Fzone1	Source4	Source1	junos-ftp junos-icmp-all junos-ntp junos-ping junos-ssh junos-tftp	Permit	Active	False	
17	279	P151	Fzone1	Source4	Source1	Source4	junos-ftp junos-icmp-all junos-ntp junos-ping junos-ssh junos-tftp	Permit	Active	False	
18	288	P57	Fzone1	Fzone1			any	Permit	Active	False	

Total 18 items.