

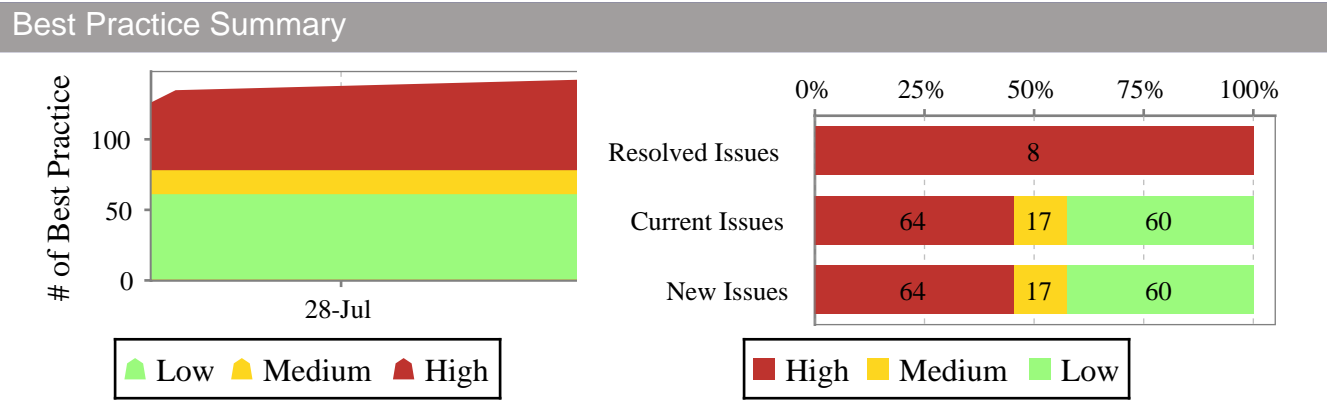
# Best Practice Changes by Device



**User Name:** uiadmin

**Parameters:** View = Subnets; Coverage Date = Jul 4, 2009, 8:44 PM (EDT) - Aug 3, 2009, 8:44 PM (EDT); Sort failure report by = first-noticed; Sort devices by = name; Include Failures = new;

**Description:** Changes in Best Practice failure instances for individual devices during a specified time period.



### Summary Data

	Devices in this report	All of network
Network Devices	14	14
Network Devices with a change	14	14
Avg. changes / Network Device	10.6	10.6
# of new Best Practice	141	141
# of fixed Best Practice	8	8

Subnets > Trusted 14 of 14 devices have changed

**B2B-ER was audited 1 time, with 20 changes, during this Period.**

New Best Practice Date	Resolved Best Practice Date	Severity	Summary	Violation ID
Jul 22 2009/16:16 PM		medium	IP Unreachables messages allowed on interface Ethernet1/0	54
Jul 22 2009/16:16 PM		low	Global service PAD enabled	55
Jul 22 2009/16:16 PM		low	Bootp server has not been disabled	56
Jul 22 2009/16:16 PM		high	No enable secret	57
Jul 22 2009/16:16 PM		high	Weak community string 'public' in command 'snmp-server community ***stripped*** RO'	58
Jul 22 2009/16:16 PM		high	Gratuitous ARP is enabled by default	59
Jul 22 2009/16:16 PM		low	Global option TCP Keepalives In is disabled	60
Jul 22 2009/16:16 PM		medium	Proxy arps are allowed	61
Jul 22 2009/16:16 PM		low	Global option TCP Keepalives Out disabled	62
Jul 22 2009/16:16 PM		high	IP source routing is enabled by default	63
Jul 22 2009/16:16 PM		medium	IP Unreachables messages allowed on interface Ethernet0/0	64
Jul 22 2009/16:16 PM		medium	Proxy arps are allowed	65
Jul 22 2009/16:28 PM	Jul 23 2009/10:16 AM	high	Untrusted rlogin access from subnet 65.173.2.8/30 to network device(s) on TCP port 513	177
Jul 22 2009/16:28 PM	Jul 23 2009/10:16 AM	high	Untrusted telnet access from subnet 65.173.2.8/30 to network device(s) on TCP port 23	178
Jul 22 2009/16:28 PM	Jul 23 2009/10:16 AM	high	Untrusted ssh access from subnet 65.173.2.8/30 to network device(s) on TCP port 22	179
Jul 22 2009/16:28 PM	Jul 23 2009/10:16 AM	high	Untrusted access to network device(s) on ICMP;TCP:port{49 161};UDP:port{67 500} from/through subnet 65.173.2.8/30	183
Jul 23 2009/10:16 AM		high	Untrusted rlogin access from subnet b2b Inet to network device(s) on TCP port 513	253
Jul 23 2009/10:16 AM		high	Untrusted telnet access from subnet b2b Inet to network device(s) on TCP port 23	254

New Best Practice Date	Resolved Best Practice Date	Severity	Summary	Violation ID
Jul 23 2009/10:16 AM		high	Untrusted ssh access from subnet b2b lnet to network device(s) on TCP port 22	255
Jul 23 2009/10:16 AM		high	Untrusted access to network device(s) on ICMP;TCP:port{49 161};UDP:port{67 500} from/through subnet b2b lnet	260

**B2B-Pix was audited 1 time, with 3 changes, during this Period.**

New Best Practice Date	Resolved Best Practice Date	Severity	Summary	Violation ID
Jul 22 2009/16:22 PM		medium	Unrestricted ICMP traffic allowed	142
Jul 22 2009/16:28 PM	Jul 23 2009/10:16 AM	high	Untrusted access to network device(s) on ICMP;TCP:port{49 161};UDP:port{67 500} from/through subnet 65.173.2.8/30	183
Jul 23 2009/10:16 AM		high	Untrusted access to network device(s) on ICMP;TCP:port{49 161};UDP:port{67 500} from/through subnet b2b lnet	260

**Hamburg was audited 1 time, with 13 changes, during this Period.**

New Best Practice Date	Resolved Best Practice Date	Severity	Summary	Violation ID
Jul 22 2009/16:16 PM		high	IP source routing is enabled by default	66
Jul 22 2009/16:16 PM		medium	Global UDP Small Servers enabled by explicit command	67
Jul 22 2009/16:16 PM		high	Weak community string 'public' in command 'snmp-server community ***stripped*** RO'	69
Jul 22 2009/16:16 PM		high	No password for user account 'username usernopasswd nopassword'	72
Jul 22 2009/16:16 PM		medium	Global TCP Small Servers enabled by explicit command	73
Jul 22 2009/16:16 PM		high	Superfluous enable password command	77
Jul 22 2009/16:16 PM		medium	Finger is enabled via command 'ip finger'	78
Jul 22 2009/16:16 PM		low	Global service TFTP is enabled	68
Jul 22 2009/16:16 PM		low	Management of device by HTTP is enabled on Hamburg	70
Jul 22 2009/16:16 PM		medium	Global service Identd enabled via command 'ip identd'	71
Jul 22 2009/16:16 PM		low	Global service PAD enabled	74
Jul 22 2009/16:16 PM		high	Gratuitous ARP is enabled by default	75
Jul 22 2009/16:16 PM		low	Bootp server has not been disabled	76

**Hamburg-NS was audited 1 time, with 11 changes, during this Period.**

New Best Practice Date	Resolved Best Practice Date	Severity	Summary	Violation ID
Jul 22 2009/16:23 PM		low	The object 'MIP(10.1.6.2)' is defined but not invoked in a policy	163
Jul 22 2009/16:23 PM		low	No console timeout (set console timeout 0 )	164
Jul 22 2009/16:23 PM		high	IP source routing is enabled for Untrust zone by explicit command	165
Jul 22 2009/16:23 PM		low	Management of device by HTTP is enabled on untrust	166
Jul 22 2009/16:23 PM		low	The telnet protocol is enabled on interface untrust	167
Jul 22 2009/16:23 PM		high	Weak community string 'public' in command 'set snmp community ***stripped*** Read-Write Trap-on version v1 '	168
Jul 22 2009/16:23 PM		high	Default password still in use	169
Jul 22 2009/16:23 PM		low	Firewall has not been configured for DNS	170
Jul 22 2009/16:23 PM		low	Traffic allowed by default (set policy default-permit-all )	171
Jul 22 2009/16:23 PM		low	Default user name 'netscreen' enabled	172
Jul 22 2009/16:23 PM		low	TCP sequence checking is disabled	173

**Karachi-CPT was audited 1 time, with 4 changes, during this Period.**

New Best Practice Date	Resolved Best Practice Date	Severity	Summary	Violation ID
Jul 22 2009/16:15 PM		medium	Stealth rule missing	50
Jul 22 2009/16:15 PM		low	VPN-1/Firewall-1/UTM implied rules enabled	51
Jul 22 2009/16:15 PM		medium	Clean-up rule missing	52
Jul 22 2009/16:15 PM		low	SmartUpdate (CPRID) implied rules enabled	53

**KarachilR was audited 1 time, with 8 changes, during this Period.**

New Best Practice Date	Resolved Best Practice Date	Severity	Summary	Violation ID
Jul 22 2009/16:16 PM		high	Gratuitous ARP is enabled by default	79
Jul 22 2009/16:16 PM		low	Bootp server has not been disabled	80
Jul 22 2009/16:16 PM		high	IP source routing is enabled by default	81
Jul 22 2009/16:16 PM		low	Global option TCP Keepalives Out disabled	82
Jul 22 2009/16:16 PM		low	Global service PAD enabled	83
Jul 22 2009/16:16 PM		low	Global option TCP Keepalives In is disabled	84
Jul 22 2009/16:16 PM		high	Weak community string 'public' in command 'snmp-server community ***stripped*** RO'	85
Jul 22 2009/16:16 PM		high	No enable secret	86

**RemoteOffices was audited 1 time, with 8 changes, during this Period.**

New Best Practice Date	Resolved Best Practice Date	Severity	Summary	Violation ID
Jul 22 2009/16:16 PM		low	Global service PAD enabled	115
Jul 22 2009/16:16 PM		low	Global option TCP Keepalives Out disabled	116
Jul 22 2009/16:16 PM		high	IP source routing is enabled by default	117
Jul 22 2009/16:16 PM		low	Global option TCP Keepalives In is disabled	118
Jul 22 2009/16:16 PM		low	Bootp server has not been disabled	119
Jul 22 2009/16:16 PM		high	Weak community string 'public' in command 'snmp-server community ***stripped*** RO'	120
Jul 22 2009/16:16 PM		high	Gratuitous ARP is enabled by default	121
Jul 22 2009/16:16 PM		high	No enable secret	122

**SM-Core was audited 1 time, with 8 changes, during this Period.**

New Best Practice Date	Resolved Best Practice Date	Severity	Summary	Violation ID
Jul 22 2009/16:16 PM		low	Global service PAD enabled	99
Jul 22 2009/16:16 PM		high	IP source routing is enabled by default	100
Jul 22 2009/16:16 PM		low	Global option TCP Keepalives In is disabled	101
Jul 22 2009/16:16 PM		high	Gratuitous ARP is enabled by default	102
Jul 22 2009/16:16 PM		low	Bootp server has not been disabled	103
Jul 22 2009/16:16 PM		high	No enable secret	104
Jul 22 2009/16:16 PM		low	Global option TCP Keepalives Out disabled	105
Jul 22 2009/16:16 PM		high	Weak community string 'public' in command 'snmp-server community ***stripped*** RO'	106

**SM-DataCenter was audited 1 time, with 8 changes, during this Period.**

New Best Practice Date	Resolved Best Practice Date	Severity	Summary	Violation ID
Jul 22 2009/16:16 PM		high	Gratuitous ARP is enabled by default	107
Jul 22 2009/16:16 PM		low	Global service PAD enabled	108
Jul 22 2009/16:16 PM		high	Weak community string 'public' in command 'snmp-server community ***stripped*** RO'	109

New Best Practice Date	Resolved Best Practice Date	Severity	Summary	Violation ID
Jul 22 2009/16:16 PM		low	Bootp server has not been disabled	110
Jul 22 2009/16:16 PM		low	Global option TCP Keepalives In is disabled	111
Jul 22 2009/16:16 PM		high	IP source routing is enabled by default	112
Jul 22 2009/16:16 PM		low	Global option TCP Keepalives Out disabled	113
Jul 22 2009/16:16 PM		high	No enable secret	114

**SM-ER was audited 1 time, with 20 changes, during this Period.**

New Best Practice Date	Resolved Best Practice Date	Severity	Summary	Violation ID
Jul 22 2009/16:16 PM		medium	IP Unreachables messages allowed on interface Ethernet1/0	87
Jul 22 2009/16:16 PM		low	Global option TCP Keepalives In is disabled	88
Jul 22 2009/16:16 PM		high	Weak community string 'public' in command 'snmp-server location San Mateo'	89
Jul 22 2009/16:16 PM		medium	IP Unreachables messages allowed on interface Ethernet0/0	90
Jul 22 2009/16:16 PM		medium	Proxy arps are allowed	91
Jul 22 2009/16:16 PM		high	No enable secret	92
Jul 22 2009/16:16 PM		low	Global service PAD enabled	93
Jul 22 2009/16:16 PM		high	Gratuitous ARP is enabled by default	94
Jul 22 2009/16:16 PM		high	IP source routing is enabled by default	95
Jul 22 2009/16:16 PM		low	Global option TCP Keepalives Out disabled	96
Jul 22 2009/16:16 PM		medium	Proxy arps are allowed	97
Jul 22 2009/16:16 PM		low	Bootp server has not been disabled	98
Jul 22 2009/16:28 PM	Jul 23 2009/10:16 AM	high	Untrusted rlogin access from subnet 4.1.1.0/30 to network device(s) on TCP port 513	174
Jul 22 2009/16:28 PM	Jul 23 2009/10:16 AM	high	Untrusted telnet access from subnet 4.1.1.0/30 to network device(s) on TCP port 23	175
Jul 22 2009/16:28 PM	Jul 23 2009/10:16 AM	high	Untrusted ssh access from subnet 4.1.1.0/30 to network device(s) on TCP port 22	176
Jul 22 2009/16:28 PM	Jul 23 2009/10:16 AM	high	Untrusted access to network device(s) on ICMP;TCP:port{49 161};UDP:port{67 500} from/through subnet 4.1.1.0/30	182
Jul 23 2009/10:16 AM		high	Untrusted rlogin access from subnet ATT ISP WAN to network device(s) on TCP port 513	250
Jul 23 2009/10:16 AM		high	Untrusted telnet access from subnet ATT ISP WAN to network device(s) on TCP port 23	251
Jul 23 2009/10:16 AM		high	Untrusted ssh access from subnet ATT ISP WAN to network device(s) on TCP port 22	252
Jul 23 2009/10:16 AM		high	Untrusted access to network device(s) on ICMP;TCP:port{49 161};UDP:port{67 500} from/through subnet ATT ISP WAN	259

**SM-Pix was audited 1 time, with 12 changes, during this Period.**

New Best Practice Date	Resolved Best Practice Date	Severity	Summary	Violation ID
Jul 22 2009/16:22 PM		low	Non-contiguous wildcard found	144
Jul 22 2009/16:22 PM		low	Non-contiguous wildcard found	146
Jul 22 2009/16:22 PM		low	Non-contiguous wildcard found	147
Jul 22 2009/16:22 PM		low	Non-contiguous wildcard found	148
Jul 22 2009/16:22 PM		medium	Unrestricted ICMP traffic allowed	151
Jul 22 2009/16:23 PM		low	Redundant rule in 'inside_access_in'	143
Jul 22 2009/16:23 PM		low	Redundant rule in 'inside_access_in'	145
Jul 22 2009/16:23 PM		low	Redundant rule in 'inside_access_in'	150
Jul 22 2009/16:23 PM		low	Redundant rule in 'inside_access_in'	149
Jul 22 2009/16:28 PM	Jul 23 2009/10:16 AM	high	Untrusted access to network device(s) on ICMP;TCP:port{49 161};UDP:port{67 500} from/through subnet 4.1.1.0/30	182
Jul 23 2009/10:16 AM		high	Untrusted access to network device(s) on ICMP from/through subnet Guest Wireless	258
Jul 23 2009/10:16 AM		high	Untrusted access to network device(s) on ICMP;TCP:port{49 161};UDP:port{67 500} from/through subnet ATT ISP WAN	259

**SM-Users was audited 1 time, with 11 changes, during this Period.**

New Best Practice Date	Resolved Best Practice Date	Severity	Summary	Violation ID
Jul 22 2009/16:16 PM		low	Global option TCP Keepalives Out disabled	123
Jul 22 2009/16:16 PM		high	Gratuitous ARP is enabled by default	124
Jul 22 2009/16:16 PM		high	IP source routing is enabled by default	125
Jul 22 2009/16:16 PM		low	Global option TCP Keepalives In is disabled	127
Jul 22 2009/16:16 PM		high	Weak community string 'public' in command 'snmp-server community ***stripped*** RO'	128
Jul 22 2009/16:16 PM		low	Global service PAD enabled	129
Jul 22 2009/16:16 PM		high	No enable secret	131
Jul 22 2009/16:16 PM		low	Bootp server has not been disabled	133
Jul 22 2009/16:16 PM		high	Rule 'config:84' of list 'managementin' permits all traffic	130
Jul 22 2009/16:16 PM		high	Rule 'config:74' of list 'user2' permits all traffic	132
Jul 22 2009/16:16 PM		high	Rule 'config:59' of list 'user1' permits all traffic	126

**Tokyo was audited 1 time, with 8 changes, during this Period.**

New Best Practice Date	Resolved Best Practice Date	Severity	Summary	Violation ID
Jul 22 2009/16:16 PM		high	Weak community string 'public' in command 'snmp-server community ***stripped*** RO'	134
Jul 22 2009/16:16 PM		high	IP source routing is enabled by default	135
Jul 22 2009/16:16 PM		low	Global service PAD enabled	136
Jul 22 2009/16:16 PM		high	Gratuitous ARP is enabled by default	137
Jul 22 2009/16:16 PM		low	Bootp server has not been disabled	138
Jul 22 2009/16:16 PM		high	No enable secret	139
Jul 22 2009/16:16 PM		low	Global option TCP Keepalives Out disabled	140
Jul 22 2009/16:16 PM		low	Global option TCP Keepalives In is disabled	141

**Tokyo-Pix was audited 1 time, with 11 changes, during this Period.**

New Best Practice Date	Resolved Best Practice Date	Severity	Summary	Violation ID
Jul 22 2009/16:23 PM		high	No password for user account 'username brian nopassword privilege 2 '	153
Jul 22 2009/16:23 PM		low	Non-contiguous wildcard found	154
Jul 22 2009/16:23 PM		high	DHCP server is enabled by 'ethernet1'	155
Jul 22 2009/16:23 PM		medium	Unrestricted ICMP traffic allowed	156
Jul 22 2009/16:23 PM		low	Floodguard is disabled	157
Jul 22 2009/16:23 PM		high	Weak community string 'cisco' in command 'snmp-server community ***stripped*** '	158
Jul 22 2009/16:23 PM		high	Default password still in use	159
Jul 22 2009/16:23 PM		low	Conduit is configured where an access-group is applied	160
Jul 22 2009/16:23 PM		low	Conduit is configured where an access-group is applied	162
Jul 22 2009/16:23 PM		low	Redundant rule in 'inside_access_in'	161
Jul 22 2009/16:23 PM		low	Redundant rule in 'outside_access_in'	152

Subnets > Untrusted > Internet

14 of 14 devices have changed

**B2B-ER was audited 1 time, with 20 changes, during this Period.**

New Best Practice Date	Resolved Best Practice Date	Severity	Summary	Violation ID
Jul 22 2009/16:16 PM		medium	IP Unreachables messages allowed on interface Ethernet1/0	54
Jul 22 2009/16:16 PM		low	Global service PAD enabled	55

New Best Practice Date	Resolved Best Practice Date	Severity	Summary	Violation ID
Jul 22 2009/16:16 PM		low	Bootp server has not been disabled	56
Jul 22 2009/16:16 PM		high	No enable secret	57
Jul 22 2009/16:16 PM		high	Weak community string 'public' in command 'snmp-server community ***stripped*** RO'	58
Jul 22 2009/16:16 PM		high	Gratuitous ARP is enabled by default	59
Jul 22 2009/16:16 PM		low	Global option TCP Keepalives In is disabled	60
Jul 22 2009/16:16 PM		medium	Proxy arps are allowed	61
Jul 22 2009/16:16 PM		low	Global option TCP Keepalives Out disabled	62
Jul 22 2009/16:16 PM		high	IP source routing is enabled by default	63
Jul 22 2009/16:16 PM		medium	IP Unreachables messages allowed on interface Ethernet0/0	64
Jul 22 2009/16:16 PM		medium	Proxy arps are allowed	65
Jul 22 2009/16:28 PM	Jul 23 2009/10:16 AM	high	Untrusted rlogin access from subnet 65.173.2.8/30 to network device(s) on TCP port 513	177
Jul 22 2009/16:28 PM	Jul 23 2009/10:16 AM	high	Untrusted telnet access from subnet 65.173.2.8/30 to network device(s) on TCP port 23	178
Jul 22 2009/16:28 PM	Jul 23 2009/10:16 AM	high	Untrusted ssh access from subnet 65.173.2.8/30 to network device(s) on TCP port 22	179
Jul 22 2009/16:28 PM	Jul 23 2009/10:16 AM	high	Untrusted access to network device(s) on ICMP;TCP:port{49 161};UDP:port{67 500} from/through subnet 65.173.2.8/30	183
Jul 23 2009/10:16 AM		high	Untrusted rlogin access from subnet b2b lnet to network device(s) on TCP port 513	253
Jul 23 2009/10:16 AM		high	Untrusted telnet access from subnet b2b lnet to network device(s) on TCP port 23	254
Jul 23 2009/10:16 AM		high	Untrusted ssh access from subnet b2b lnet to network device(s) on TCP port 22	255
Jul 23 2009/10:16 AM		high	Untrusted access to network device(s) on ICMP;TCP:port{49 161};UDP:port{67 500} from/through subnet b2b lnet	260

**SM-ER was audited 1 time, with 20 changes, during this Period.**

New Best Practice Date	Resolved Best Practice Date	Severity	Summary	Violation ID
Jul 22 2009/16:16 PM		medium	IP Unreachables messages allowed on interface Ethernet1/0	87
Jul 22 2009/16:16 PM		low	Global option TCP Keepalives In is disabled	88
Jul 22 2009/16:16 PM		high	Weak community string 'public' in command 'snmp-server location San Mateo'	89
Jul 22 2009/16:16 PM		medium	IP Unreachables messages allowed on interface Ethernet0/0	90
Jul 22 2009/16:16 PM		medium	Proxy arps are allowed	91
Jul 22 2009/16:16 PM		high	No enable secret	92
Jul 22 2009/16:16 PM		low	Global service PAD enabled	93
Jul 22 2009/16:16 PM		high	Gratuitous ARP is enabled by default	94
Jul 22 2009/16:16 PM		high	IP source routing is enabled by default	95
Jul 22 2009/16:16 PM		low	Global option TCP Keepalives Out disabled	96
Jul 22 2009/16:16 PM		medium	Proxy arps are allowed	97
Jul 22 2009/16:16 PM		low	Bootp server has not been disabled	98
Jul 22 2009/16:28 PM	Jul 23 2009/10:16 AM	high	Untrusted rlogin access from subnet 4.1.1.0/30 to network device(s) on TCP port 513	174
Jul 22 2009/16:28 PM	Jul 23 2009/10:16 AM	high	Untrusted telnet access from subnet 4.1.1.0/30 to network device(s) on TCP port 23	175
Jul 22 2009/16:28 PM	Jul 23 2009/10:16 AM	high	Untrusted ssh access from subnet 4.1.1.0/30 to network device(s) on TCP port 22	176
Jul 22 2009/16:28 PM	Jul 23 2009/10:16 AM	high	Untrusted access to network device(s) on ICMP;TCP:port{49 161};UDP:port{67 500} from/through subnet 4.1.1.0/30	182
Jul 23 2009/10:16 AM		high	Untrusted rlogin access from subnet ATT ISP WAN to network device(s) on TCP port 513	250
Jul 23 2009/10:16 AM		high	Untrusted telnet access from subnet ATT ISP WAN to network device(s) on TCP port 23	251
Jul 23 2009/10:16 AM		high	Untrusted ssh access from subnet ATT ISP WAN to network device(s) on TCP port 22	252
Jul 23 2009/10:16 AM		high	Untrusted access to network device(s) on ICMP;TCP:port{49 161};UDP:port{67 500} from/through subnet ATT ISP WAN	259

Subnets > Untrusted > Local Untrusted

14 of 14 devices have changed

**SM-Pix was audited 1 time, with 12 changes, during this Period.**

New Best Practice Date	Resolved Best Practice Date	Severity	Summary	Violation ID
Jul 22 2009/16:22 PM		low	Non-contiguous wildcard found	144
Jul 22 2009/16:22 PM		low	Non-contiguous wildcard found	146
Jul 22 2009/16:22 PM		low	Non-contiguous wildcard found	147
Jul 22 2009/16:22 PM		low	Non-contiguous wildcard found	148
Jul 22 2009/16:22 PM		medium	Unrestricted ICMP traffic allowed	151
Jul 22 2009/16:23 PM		low	Redundant rule in 'inside_access_in'	143
Jul 22 2009/16:23 PM		low	Redundant rule in 'inside_access_in'	145
Jul 22 2009/16:23 PM		low	Redundant rule in 'inside_access_in'	150
Jul 22 2009/16:23 PM		low	Redundant rule in 'inside_access_in'	149
Jul 22 2009/16:28 PM	Jul 23 2009/10:16 AM	high	Untrusted access to network device(s) on ICMP;TCP:port{49 161};UDP:port{67 500} from/through subnet 4.1.1.0/30	182
Jul 23 2009/10:16 AM		high	Untrusted access to network device(s) on ICMP from/through subnet Guest Wireless	258
Jul 23 2009/10:16 AM		high	Untrusted access to network device(s) on ICMP;TCP:port{49 161};UDP:port{67 500} from/through subnet ATT ISP WAN	259