

Firewall Migration Analysis Detail Report

Source host:abccompany-pix
Target host:migrated_sjpix
Policy package:Migrated_Policy

Completed on Tue Jul 07 12:53:13 CDT 2009

This report provides support for migrating Cisco device configurations to equivalent Checkpoint device configurations. Based on the data and recommendations provided in this report it will be possible to manually create a Checkpoint configuration that is equivalent to the Cisco original.

This report is organized by the Checkpoint rules that need to be modified to ensure that policies are identical to the Cisco firewall policies. Each Checkpoint rule is associated with a category and an explanation of the cause of policy difference for better understanding. For each such Checkpoint rule, an exact match Cisco rule or a set of overlap Cisco rules are reported, if found. These rules can be used to correct any potential mis-translations. If there are no mis-translations, two remedies to correct the policy difference are presented. These are based on Allow Policy Table and Policy Difference Table respectively. The remedy based on Allow Policy Table consists of replacing the Checkpoint rule with allow rules, while the remedy based on Policy Difference Table involves adding a set of allow or deny rules above the Checkpoint rule.

The report does not provide Checkpoint object definitions. These have to be manually created through the Checkpoint Management Console.

[Policies to and from Cisco Device](#) table shows the allow policies to and from the Cisco device. The migration report does not address migrating these policies, because Cisco and Checkpoint management protocols may be incompatible. The Policies to and from Cisco device should be reviewed and policies that need to be migrated should be done so manually.

Four additional reports are also generated.

The [Policy Difference](#) report provides policy difference between Checkpoint configuration and Cisco configuration. This report is a comprehensive listing of all policy difference items described by sources, destinations, and services.

The [Policy Difference Rule Trails](#) report shows rule trails for policy difference items listed in the Policy Difference report. This report shows the rules which are responsible for the policy difference. For each policy difference item, it provides rules from Checkpoint device as well as the rules from Cisco device.

The [Cisco Firewall Configuration](#) report is for Cisco firewall configuration and is used to view the individual Cisco rules via hyperlinks from other reports.

The [Checkpoint Firewall Configuration](#) report is for Checkpoint firewall configuration and is used to view the individual Checkpoint rules via hyperlinks from other reports.

Use Alt-left arrow to return to the source of the hyperlink.

Checkpoint Rules To Be Fixed

Index	Checkpoint rule to be fixed
1	Deleted policy caused by Checkpoint client-nat/Default-Accept rule
2	Added policy caused by Checkpoint acl rule 1
3	Added policy caused by Checkpoint acl rule 2
4	Added policy caused by Checkpoint acl rule 3
5	Added policy caused by Checkpoint acl rule 6
6	Added policy caused by Checkpoint acl rule 7
7	Added policy caused by Checkpoint acl rule 8
8	Added policy caused by Checkpoint acl rule 9
9	Added policy caused by Checkpoint acl rule 10
10	Added policy caused by Checkpoint acl rule 11
11	Added policy caused by Checkpoint acl rule 12
12	Added policy caused by Checkpoint acl rule 13
13	Added policy caused by Checkpoint acl rule 14
14	Added policy caused by Checkpoint acl rule 15
15	Added policy caused by Checkpoint acl rule 16
16	Added policy caused by Checkpoint acl rule 17
17	Added policy caused by Checkpoint acl rule 18
18	Added policy caused by Checkpoint acl rule 21
19	Added policy caused by Checkpoint acl rule 22
20	Added policy caused by Checkpoint acl rule 23
21	Added policy caused by Checkpoint acl rule 24
22	Added policy caused by Checkpoint acl rule 25
23	Added policy caused by Checkpoint acl rule 26
24	Added policy caused by Checkpoint acl rule 27
25	Added policy caused by Checkpoint acl rule 28
26	Added policy caused by Checkpoint acl rule 29
27	Added policy caused by Checkpoint acl rule 34
28	Deleted policy caused by Checkpoint acl rule 35
29	Added policy caused by Checkpoint acl rule 37
30	Added policy caused by Checkpoint acl rule 38
31	Added policy caused by Checkpoint acl rule 39
32	Added policy caused by Checkpoint acl rule 41
33	Added policy caused by Checkpoint acl rule 42
34	Added policy caused by Checkpoint acl rule 43
35	Added policy caused by Checkpoint acl rule 44
36	Added policy caused by Checkpoint acl rule 46
37	Added policy caused by Checkpoint acl rule 47
38	Added policy caused by Checkpoint acl rule 48
39	Deleted policy caused by Checkpoint acl rule 49
40	Added policy caused by Checkpoint acl rule 50
41	Added policy caused by Checkpoint acl rule 51

Index	Checkpoint rule to be fixed
42	Added policy caused by Checkpoint acl rule 52
43	Added policy caused by Checkpoint acl rule 53
44	Added policy caused by Checkpoint acl rule 54
45	Added policy caused by Checkpoint acl rule 55
46	Added policy caused by Checkpoint acl rule 56
47	Deleted policy caused by Checkpoint acl rule 57
48	Deleted policy caused by Checkpoint acl rule 76
49	Deleted policy caused by Checkpoint acl rule 77

Deleted policy caused by Checkpoint client-nat/Default-Accept rule

Rule Index	Source	Destination	Service	VPN	Action	Comment
client-nat/Default-Accept					accept	

Difference caused by:

NAT

Problem Source:

Improperly translated or out of sequence NAT rule

Remedy:

Translate NAT rules in accordance with the NAT table described at the end of the report.

Refer to [Proposed Checkpoint NAT Table](#)

Remedy based on policy diff items:

No policy difference-based remedy can be applicable for this Checkpoint rule. The policy difference table shown below is provided for additional information regarding Cisco NAT rules that are responsible for the policy differences.

Policy Difference Table:

Policy Diff Item	Source	Destination	Service	Cisco Rule Trails
546	127.0.0.1	62.59.14.169	icmp	nat:184
555	127.0.0.1	62.59.14.161	tcp/http	nat:185
556	127.0.0.1	62.59.14.169	tcp/http	nat:184
569	127.0.0.1	62.59.14.161	tcp/https	nat:185
570	127.0.0.1	62.59.14.169	tcp/https	nat:184
579	207.135.79.64	62.59.14.169	tcp/pds	nat:184
581	64.92.205.64/27	62.59.14.163	tcp/smtp	nat:181
582	66.179.26.128/26	62.59.14.163	tcp/smtp	nat:181
583	66.179.109.160/27	62.59.14.163	tcp/smtp	nat:181
584	207.38.18.128/27	62.59.14.163	tcp/smtp	nat:181
585	208.65.144.0/21	62.59.14.163	tcp/smtp	nat:181
586	216.74.18.32/27	62.59.14.163	tcp/smtp	nat:181
587	216.183.119.96/27	62.59.14.163	tcp/smtp	nat:181
591	127.0.0.1	62.59.14.171	tcp/ssh	nat:183
598	127.0.0.1	62.59.14.171	tcp/http	nat:183
605	127.0.0.1	62.59.14.171	tcp/https	nat:183
610	69.237.83.3	62.59.14.171	tcp/cbt	nat:183

Added policy caused by Checkpoint acl rule 1

Rule Index	Source	Destination	Service	VPN	Action	Comment
1	Migrated_inside_Interface	Any	http		accept	(Original ACE (line 58): access-list acl_inside permit tcp any any eq www)

Cisco Overlap Rules:

Line No	Interface	Rule
	vpn4	high-to-low-default-allow
102	testweb	access-list acl_testweb permit tcp any any eq www
109	proxymail	access-list acl_proxymail permit tcp any any eq www
35	outside	access-list acl_outside permit tcp any host 62.59.14.161 eq www
40	outside	access-list acl_outside permit tcp any host 62.59.14.170 eq www
41	outside	access-list acl_outside permit tcp any host 62.59.14.171 eq www
52	outside	access-list acl_outside permit tcp any host 62.59.14.169 eq www
56	mail1	access-list acl_mail1 permit tcp any any eq www
58	inside	access-list acl_inside permit tcp any any eq www

Difference caused by:

NAT control in Cisco Device

Problem Source:

NAT control in Cisco devices limits access to packets which are associated with NAT rules. Thus, the source, destination addresses, or services of allowed packets are smaller than what is indicated by this Checkpoint rule.

Remedy based on allow policies:

The set of packets that are allowed in the Cisco device are shown in the Allow Policy Table. To use this table:

1. Replace this Checkpoint rule with allow rules for packets described in each row of the table.
2. Use rule reduction techniques such as address aggregation, or object grouping to reduce the number of rules to be added.

Allow Policy Table:

Service	Source	Destination
tcp/http	10.0.0.0/8	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 255.255.255.255
tcp/http	172.16.0.0/15	0.0.0.0 to 9.255.255.255 11.0.0.0 to 172.15.255.255 192.168.6.0 to 192.168.8.255 192.168.10.0 to 255.255.255.255
tcp/http	172.16.0.0/16	172.18.0.0 to 192.168.1.255
tcp/http	172.17.0.0/16	172.18.0.0 to 192.168.0.255
tcp/http	192.168.2.0 to 192.168.5.255	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
tcp/http	192.168.2.0/23	192.168.10.0 to 255.255.255.255
tcp/http	192.168.4.0/23	192.168.10.0 to 192.168.49.255 192.168.51.0 to 255.255.255.255

Remedy based on policy diff items:

The set of packets that are allowed by the Checkpoint device, but denied by the Cisco device, are shown in the Policy Difference Table. There may be multiple tables, each caused by a specific problem. The remedy is the following:

1. The Checkpoint rule should not be removed or altered.
2. Add rules above this Checkpoint rule to deny each packet described in the Policy Difference Table below.
3. Use rule reduction techniques such as address aggregation, or object grouping to reduce the number of rules to be added

Policy Difference Table:

Policy Diff Item	Source	Destination	Service	Cisco Rule Trails
------------------	--------	-------------	---------	-------------------

Policy Diff Item	Source	Destination	Service	Cisco Rule Trails
156	10.0.0.0/8	192.168.9.0/24	tcp/http	nat:nat/Default-Deny
176	172.16.0.0/16	192.168.9.0/24	tcp/http	nat:nat/Default-Deny
176	172.17.0.0/16	192.168.9.0/24	tcp/http	nat:nat/Default-Deny
194	192.168.5.0/24	192.168.9.0/24	tcp/http	nat:nat/Default-Deny
194	192.168.3.0/24	192.168.9.0/24	tcp/http	nat:nat/Default-Deny
194	192.168.2.0/24	192.168.9.0/24	tcp/http	nat:nat/Default-Deny
194	192.168.4.0/24	192.168.9.0/24	tcp/http	nat:nat/Default-Deny
223	10.0.0.0/8	192.168.1.0/24	tcp/http	nat:nat/Default-Deny
224	172.17.0.0/16	192.168.1.0/24	tcp/http	nat:nat/Default-Deny
225	192.168.5.0/24	192.168.1.0/24	tcp/http	nat:nat/Default-Deny
225	192.168.2.0/24	192.168.1.0/24	tcp/http	nat:nat/Default-Deny
225	192.168.4.0/24	192.168.1.0/24	tcp/http	nat:nat/Default-Deny
225	192.168.3.0/24	192.168.1.0/24	tcp/http	nat:nat/Default-Deny
268	192.168.4.0/24	192.168.50.0/24	tcp/http	nat:nat/Default-Deny
268	192.168.5.0/24	192.168.50.0/24	tcp/http	nat:nat/Default-Deny

Added policy caused by Checkpoint acl rule 2

Rule Index	Source	Destination	Service	VPN	Action	Comment
2	Migrated_inside_Interface	Any	https		accept	(Original ACE (line 59): access-list acl_inside permit tcp any any eq https)

Cisco Overlap Rules:

Line No	Interface	Rule
	vpn4	high-to-low-default-allow
103	testweb	access-list acl_testweb permit tcp any any eq https
110	proxymail	access-list acl_proxymail permit tcp any any eq https
36	outside	access-list acl_outside permit tcp any host 62.59.14.161 eq https
42	outside	access-list acl_outside permit tcp any host 62.59.14.171 eq https
51	outside	access-list acl_outside permit tcp any host 62.59.14.169 eq https
57	mail1	access-list acl_mail1 permit tcp any any eq https
59	inside	access-list acl_inside permit tcp any any eq https

Difference caused by:

NAT control in Cisco Device

Problem Source:

NAT control in Cisco devices limits access to packets which are associated with NAT rules. Thus, the source, destination addresses, or services of allowed packets are smaller than what is indicated by this Checkpoint rule.

Remedy based on allow policies:

The set of packets that are allowed in the Cisco device are shown in the Allow Policy Table. To use this table:

1. Replace this Checkpoint rule with allow rules for packets described in each row of the table.
2. Use rule reduction techniques such as address aggregation, or object grouping to reduce the number of rules to be added.

Allow Policy Table:

Service	Source	Destination
tcp/https	10.0.0.0/8	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 255.255.255.255
tcp/https	172.16.0.0/15	0.0.0.0 to 9.255.255.255 11.0.0.0 to 172.15.255.255 192.168.6.0 to 192.168.8.255 192.168.10.0 to 255.255.255.255
tcp/https	172.16.0.0/16	172.18.0.0 to 192.168.1.255
tcp/https	172.16.0.101 172.16.0.200 172.16.6.44 172.16.31.46	172.16.0.1
tcp/https	172.17.0.0/16	172.18.0.0 to 192.168.0.255
tcp/https	192.168.2.0 to 192.168.5.255	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
tcp/https	192.168.2.0/23	192.168.10.0 to 255.255.255.255
tcp/https	192.168.4.0/23	192.168.10.0 to 192.168.49.255 192.168.51.0 to 255.255.255.255

Remedy based on policy diff items:

The set of packets that are allowed by the Checkpoint device, but denied by the Cisco device, are shown in the Policy Difference Table. There may be multiple tables, each caused by a specific problem. The remedy is the following:

1. The Checkpoint rule should not be removed or altered.
2. Add rules above this Checkpoint rule to deny each packet described in the Policy Difference Table below.
3. Use rule reduction techniques such as address aggregation, or object grouping to reduce the number of rules to be added

Policy Difference Table:

Policy Diff Item	Source	Destination	Service	Cisco Rule Trails
158	10.0.0.0/8	192.168.9.0/24	tcp/https	nat:nat/Default-Deny
178	172.16.0.0/15	192.168.9.0/24	tcp/https	nat:nat/Default-Deny
196	192.168.2.0 to 192.168.5.255	192.168.9.0/24	tcp/https	nat:nat/Default-Deny
229	10.0.0.0/8	192.168.1.0/24	tcp/https	nat:nat/Default-Deny
230	172.17.0.0/16	192.168.1.0/24	tcp/https	nat:nat/Default-Deny
231	192.168.2.0 to 192.168.5.255	192.168.1.0/24	tcp/https	nat:nat/Default-Deny
270	192.168.4.0/23	192.168.50.0/24	tcp/https	nat:nat/Default-Deny

Added policy caused by Checkpoint acl rule 3

Rule Index	Source	Destination	Service	VPN	Action	Comment
3	Migrated_inside_Interface	Any	netsupport		accept	(Original ACE (line 60): access-list acl_inside permit tcp any any eq 5405)

Cisco Overlap Rules:

Line No	Interface	Rule
	vpn4	high-to-low-default-allow
60	inside	access-list acl_inside permit tcp any any eq 5405

Difference caused by:

NAT control in Cisco Device

Problem Source:

NAT control in Cisco devices limits access to packets which are associated with NAT rules. Thus, the source, destination addresses, or services of allowed packets are smaller than what is indicated by this Checkpoint rule.

Remedy based on allow policies:

The set of packets that are allowed in the Cisco device are shown in the Allow Policy Table. To use this table:

1. Replace this Checkpoint rule with allow rules for packets described in each row of the table.
2. Use rule reduction techniques such as address aggregation, or object grouping to reduce the number of rules to be added.

Allow Policy Table:

Service	Source	Destination
tcp/netsupport	10.0.0.0/8	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 255.255.255.255
tcp/netsupport	172.16.0.0/15	0.0.0.0 to 9.255.255.255 11.0.0.0 to 172.15.255.255 192.168.6.0 to 192.168.8.255 192.168.10.0 to 255.255.255.255
tcp/netsupport	172.16.0.0/16	172.18.0.0 to 192.168.1.255
tcp/netsupport	172.17.0.0/16	172.18.0.0 to 192.168.0.255
tcp/netsupport	192.168.2.0 to 192.168.5.255	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
tcp/netsupport	192.168.2.0/23	192.168.10.0 to 255.255.255.255
tcp/netsupport	192.168.4.0/23	192.168.10.0 to 192.168.49.255 192.168.51.0 to 255.255.255.255

Remedy based on policy diff items:

The set of packets that are allowed by the Checkpoint device, but denied by the Cisco device, are shown in the Policy Difference Table. There may be multiple tables, each caused by a specific problem. The remedy is the following:

1. The Checkpoint rule should not be removed or altered.
2. Add rules above this Checkpoint rule to deny each packet described in the Policy Difference Table below.
3. Use rule reduction techniques such as address aggregation, or object grouping to reduce the number of rules to be added

Policy Difference Table:

Policy Diff Item	Source	Destination	Service	Cisco Rule Trails
160	10.0.0.0/8	192.168.9.0/24	tcp/netsupport	nat:nat/Default-Deny
180	172.16.0.0/15	192.168.9.0/24	tcp/netsupport	nat:nat/Default-Deny
198	192.168.2.0 to 192.168.5.255	192.168.9.0/24	tcp/netsupport	nat:nat/Default-Deny
235	10.0.0.0/8	192.168.1.0/24	tcp/netsupport	nat:nat/Default-Deny
236	172.17.0.0/16	192.168.1.0/24	tcp/netsupport	nat:nat/Default-Deny
237	192.168.2.0 to 192.168.5.255	192.168.1.0/24	tcp/netsupport	nat:nat/Default-Deny
274	192.168.4.0/23	192.168.50.0/24	tcp/netsupport	nat:nat/Default-Deny

Added policy caused by Checkpoint acl rule 6

Rule Index	Source	Destination	Service	VPN	Action	Comment
6	Migrated_inside_Interface	Any	ftp		accept	(Original ACE (line 63): access-list acl_inside permit tcp any any eq ftp)

Cisco Overlap Rules:

Line No	Interface	Rule
	vpn4	high-to-low-default-allow
63	inside	access-list acl_inside permit tcp any any eq ftp

Difference caused by:

NAT control in Cisco Device

Problem Source:

NAT control in Cisco devices limits access to packets which are associated with NAT rules. Thus, the source, destination addresses, or services of allowed packets are smaller than what is indicated by this Checkpoint rule.

Remedy based on allow policies:

The set of packets that are allowed in the Cisco device are shown in the Allow Policy Table. To use this table:

1. Replace this Checkpoint rule with allow rules for packets described in each row of the table.
2. Use rule reduction techniques such as address aggregation, or object grouping to reduce the number of rules to be added.

Allow Policy Table:

Service	Source	Destination
tcp/ftp	10.0.0.0/8	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 255.255.255.255
tcp/ftp	172.16.0.0 to 172.16.0.23	0.0.0.0 to 9.255.255.255 11.0.0.0 to 172.15.255.255 172.18.0.0 to 192.168.1.255 192.168.6.0 to 192.168.8.255 192.168.10.0 to 255.255.255.255
tcp/ftp	172.16.0.25 to 172.17.255.255	0.0.0.0 to 9.255.255.255 11.0.0.0 to 172.15.255.255 192.168.6.0 to 192.168.8.255 192.168.10.0 to 255.255.255.255
tcp/ftp	172.16.0.25 to 172.16.255.255	172.18.0.0 to 192.168.1.255
tcp/ftp	172.17.0.0/16	172.18.0.0 to 192.168.0.255
tcp/ftp	192.168.2.0 to 192.168.5.255	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

Service	Source	Destination
tcp/ftp	192.168.2.0 to 192.168.5.255	192.168.6.0 to 192.168.8.255
tcp/ftp	192.168.2.0/23	192.168.10.0 to 255.255.255.255
tcp/ftp	192.168.4.0/23	192.168.10.0 to 192.168.49.255 192.168.51.0 to 255.255.255.255

Remedy based on policy diff items:

The set of packets that are allowed by the Checkpoint device, but denied by the Cisco device, are shown in the Policy Difference Table. There may be multiple tables, each caused by a specific problem. The remedy is the following:

1. The Checkpoint rule should not be removed or altered.
2. Add rules above this Checkpoint rule to deny each packet described in the Policy Difference Table below.
3. Use rule reduction techniques such as address aggregation, or object grouping to reduce the number of rules to be added

Policy Difference Table:

Policy Diff Item	Source	Destination	Service	Cisco Rule Trails
155	10.0.0.0/8	192.168.9.0/24	tcp/ftp	nat:nat/Default-Deny
168	172.16.0.0 to 172.16.0.23	192.168.9.0/24	tcp/ftp	nat:nat/Default-Deny
187	172.17.0.0/16	192.168.9.0/24	tcp/ftp	nat:nat/Default-Deny
187	172.16.0.25 to 172.16.255.255	192.168.9.0/24	tcp/ftp	nat:nat/Default-Deny
193	192.168.4.0/24	192.168.9.0/24	tcp/ftp	nat:nat/Default-Deny
193	192.168.5.0/24	192.168.9.0/24	tcp/ftp	nat:nat/Default-Deny
193	192.168.3.0/24	192.168.9.0/24	tcp/ftp	nat:nat/Default-Deny
193	192.168.2.0/24	192.168.9.0/24	tcp/ftp	nat:nat/Default-Deny
220	10.0.0.0/8	192.168.1.0/24	tcp/ftp	nat:nat/Default-Deny
221	172.17.0.0/16	192.168.1.0/24	tcp/ftp	nat:nat/Default-Deny
222	192.168.3.0/24	192.168.1.0/24	tcp/ftp	nat:nat/Default-Deny
222	192.168.4.0/24	192.168.1.0/24	tcp/ftp	nat:nat/Default-Deny
222	192.168.5.0/24	192.168.1.0/24	tcp/ftp	nat:nat/Default-Deny
222	192.168.2.0/24	192.168.1.0/24	tcp/ftp	nat:nat/Default-Deny
267	192.168.4.0/24	192.168.50.0/24	tcp/ftp	nat:nat/Default-Deny
267	192.168.5.0/24	192.168.50.0/24	tcp/ftp	nat:nat/Default-Deny

Added policy caused by Checkpoint acl rule 7

Rule Index	Source	Destination	Service	VPN	Action	Comment
7	Migrated_inside_Interface	Any	ssh		accept	(Original ACE (line 64): access-list acl_inside permit tcp any any eq ssh)

Cisco Overlap Rules:

Line No	Interface	Rule
	vpn4	high-to-low-default-allow
104	testweb	access-list acl_testweb permit tcp any any eq ssh
43	outside	access-list acl_outside permit tcp any host 62.59.14.171 eq ssh
64	inside	access-list acl_inside permit tcp any any eq ssh

Difference caused by:

NAT control in Cisco Device

Problem Source:

NAT control in Cisco devices limits access to packets which are associated with NAT rules. Thus, the source, destination addresses, or services of allowed packets are smaller than what is indicated by this Checkpoint rule.

Remedy based on allow policies:

The set of packets that are allowed in the Cisco device are shown in the Allow Policy Table. To use this table:

1. Replace this Checkpoint rule with allow rules for packets described in each row of the table.
2. Use rule reduction techniques such as address aggregation, or object grouping to reduce the number of rules to be added.

Allow Policy Table:

Service	Source	Destination
tcp/ssh	10.0.0.0/8	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 255.255.255.255
tcp/ssh	172.16.0.0 to 172.16.0.23	0.0.0.0 to 9.255.255.255 11.0.0.0 to 172.15.255.255 172.18.0.0 to 192.168.1.255 192.168.6.0 to 192.168.8.255 192.168.10.0 to 255.255.255.255
tcp/ssh	172.16.0.25 to 172.17.255.255	0.0.0.0 to 9.255.255.255 11.0.0.0 to 172.15.255.255 192.168.6.0 to 192.168.8.255 192.168.10.0 to 255.255.255.255
tcp/ssh	172.16.0.25 to 172.16.255.255	172.18.0.0 to 192.168.1.255
tcp/ssh	172.17.0.0/16	172.18.0.0 to 192.168.0.255

Service	Source	Destination
tcp/ssh	192.168.2.0 to 192.168.5.255	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
tcp/ssh	192.168.2.0/23	192.168.10.0 to 255.255.255.255
tcp/ssh	192.168.4.0/23	192.168.10.0 to 192.168.49.255 192.168.51.0 to 255.255.255.255

Remedy based on policy diff items:

The set of packets that are allowed by the Checkpoint device, but denied by the Cisco device, are shown in the Policy Difference Table. There may be multiple tables, each caused by a specific problem. The remedy is the following:

1. The Checkpoint rule should not be removed or altered.
2. Add rules above this Checkpoint rule to deny each packet described in the Policy Difference Table below.
3. Use rule reduction techniques such as address aggregation, or object grouping to reduce the number of rules to be added

Policy Difference Table:

Policy Diff Item	Source	Destination	Service	Cisco Rule Trails
155	10.0.0.0/8	192.168.9.0/24	tcp/ssh	nat:nat/Default-Deny
168	172.16.0.0 to 172.16.0.23	192.168.9.0/24	tcp/ssh	nat:nat/Default-Deny
187	172.17.0.0/16	192.168.9.0/24	tcp/ssh	nat:nat/Default-Deny
187	172.16.0.25 to 172.16.255.255	192.168.9.0/24	tcp/ssh	nat:nat/Default-Deny
193	192.168.4.0/24	192.168.9.0/24	tcp/ssh	nat:nat/Default-Deny
193	192.168.2.0/24	192.168.9.0/24	tcp/ssh	nat:nat/Default-Deny
193	192.168.3.0/24	192.168.9.0/24	tcp/ssh	nat:nat/Default-Deny
193	192.168.5.0/24	192.168.9.0/24	tcp/ssh	nat:nat/Default-Deny
220	10.0.0.0/8	192.168.1.0/24	tcp/ssh	nat:nat/Default-Deny
221	172.17.0.0/16	192.168.1.0/24	tcp/ssh	nat:nat/Default-Deny
222	192.168.2.0/24	192.168.1.0/24	tcp/ssh	nat:nat/Default-Deny
222	192.168.3.0/24	192.168.1.0/24	tcp/ssh	nat:nat/Default-Deny
222	192.168.5.0/24	192.168.1.0/24	tcp/ssh	nat:nat/Default-Deny
222	192.168.4.0/24	192.168.1.0/24	tcp/ssh	nat:nat/Default-Deny
267	192.168.5.0/24	192.168.50.0/24	tcp/ssh	nat:nat/Default-Deny
267	192.168.4.0/24	192.168.50.0/24	tcp/ssh	nat:nat/Default-Deny

Added policy caused by Checkpoint acl rule 8

Rule Index	Source	Destination	Service	VPN	Action	Comment
8	Migrated_inside_Interface	Any	hosts2-ns		accept	(Original ACE (line 65): access-list acl_inside permit tcp any any eq 81)

Cisco Overlap Rules:

Line No	Interface	Rule
	vpn4	high-to-low-default-allow
65	inside	access-list acl_inside permit tcp any any eq 81

Difference caused by:

NAT control in Cisco Device

Problem Source:

NAT control in Cisco devices limits access to packets which are associated with NAT rules. Thus, the source, destination addresses, or services of allowed packets are smaller than what is indicated by this Checkpoint rule.

Remedy based on allow policies:

The set of packets that are allowed in the Cisco device are shown in the Allow Policy Table. To use this table:

1. Replace this Checkpoint rule with allow rules for packets described in each row of the table.
2. Use rule reduction techniques such as address aggregation, or object grouping to reduce the number of rules to be added.

Allow Policy Table:

Service	Source	Destination
tcp/hosts2-ns	10.0.0.0/8	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 255.255.255.255
tcp/hosts2-ns	172.16.0.0/15	0.0.0.0 to 9.255.255.255 11.0.0.0 to 172.15.255.255 192.168.6.0 to 192.168.8.255 192.168.10.0 to 255.255.255.255
tcp/hosts2-ns	172.16.0.0/16	172.18.0.0 to 192.168.1.255
tcp/hosts2-ns	172.17.0.0/16	172.18.0.0 to 192.168.0.255
tcp/hosts2-ns	192.168.2.0 to 192.168.5.255	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
tcp/hosts2-ns	192.168.2.0/23	192.168.10.0 to 255.255.255.255
tcp/hosts2-ns	192.168.4.0/23	192.168.10.0 to 192.168.49.255 192.168.51.0 to 255.255.255.255

Remedy based on policy diff items:

The set of packets that are allowed by the Checkpoint device, but denied by the Cisco device, are shown in the Policy Difference Table. There may be multiple tables, each caused by a specific problem. The remedy is the following:

1. The Checkpoint rule should not be removed or altered.
2. Add rules above this Checkpoint rule to deny each packet described in the Policy Difference Table below.
3. Use rule reduction techniques such as address aggregation, or object grouping to reduce the number of rules to be added

Policy Difference Table:

Policy Diff Item	Source	Destination	Service	Cisco Rule Trails
156	10.0.0.0/8	192.168.9.0/24	tcp/hosts2-ns	nat:nat/Default-Deny
176	172.17.0.0/16	192.168.9.0/24	tcp/hosts2-ns	nat:nat/Default-Deny
176	172.16.0.0/16	192.168.9.0/24	tcp/hosts2-ns	nat:nat/Default-Deny
194	192.168.4.0/24	192.168.9.0/24	tcp/hosts2-ns	nat:nat/Default-Deny
194	192.168.2.0/24	192.168.9.0/24	tcp/hosts2-ns	nat:nat/Default-Deny
194	192.168.3.0/24	192.168.9.0/24	tcp/hosts2-ns	nat:nat/Default-Deny
194	192.168.5.0/24	192.168.9.0/24	tcp/hosts2-ns	nat:nat/Default-Deny
223	10.0.0.0/8	192.168.1.0/24	tcp/hosts2-ns	nat:nat/Default-Deny
224	172.17.0.0/16	192.168.1.0/24	tcp/hosts2-ns	nat:nat/Default-Deny
225	192.168.4.0/24	192.168.1.0/24	tcp/hosts2-ns	nat:nat/Default-Deny
225	192.168.2.0/24	192.168.1.0/24	tcp/hosts2-ns	nat:nat/Default-Deny
225	192.168.5.0/24	192.168.1.0/24	tcp/hosts2-ns	nat:nat/Default-Deny
225	192.168.3.0/24	192.168.1.0/24	tcp/hosts2-ns	nat:nat/Default-Deny
268	192.168.5.0/24	192.168.50.0/24	tcp/hosts2-ns	nat:nat/Default-Deny
268	192.168.4.0/24	192.168.50.0/24	tcp/hosts2-ns	nat:nat/Default-Deny

Added policy caused by Checkpoint acl rule 9

Rule Index	Source	Destination	Service	VPN	Action	Comment
9	Migrated_inside_Interface	Any	telnet		accept	(Original ACE (line 66): access-list acl_inside permit tcp any any eq telnet)

Cisco Overlap Rules:

Line No	Interface	Rule
	vpn4	high-to-low-default-allow
66	inside	access-list acl_inside permit tcp any any eq telnet

Difference caused by:

NAT control in Cisco Device

Problem Source:

NAT control in Cisco devices limits access to packets which are associated with NAT rules. Thus, the source, destination addresses, or services of allowed packets are smaller than what is indicated by this Checkpoint rule.

Remedy based on allow policies:

The set of packets that are allowed in the Cisco device are shown in the Allow Policy Table. To use this table:

1. Replace this Checkpoint rule with allow rules for packets described in each row of the table.
2. Use rule reduction techniques such as address aggregation, or object grouping to reduce the number of rules to be added.

Allow Policy Table:

Service	Source	Destination
tcp/telnet	10.0.0.0/8	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 255.255.255.255
tcp/telnet	172.16.0.0/15	0.0.0.0 to 9.255.255.255 11.0.0.0 to 172.15.255.255 192.168.6.0 to 192.168.8.255 192.168.10.0 to 255.255.255.255
tcp/telnet	172.16.0.0/16	172.16.0.1 172.18.0.0 to 192.168.1.255
tcp/telnet	172.17.0.0/16	172.18.0.0 to 192.168.0.255
tcp/telnet	192.168.2.0 to 192.168.5.255	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
tcp/telnet	192.168.2.0/23	192.168.10.0 to 255.255.255.255
tcp/telnet	192.168.3.0/24	172.16.0.1
tcp/telnet	192.168.4.0/23	192.168.10.0 to 192.168.49.255 192.168.51.0 to 255.255.255.255

Remedy based on policy diff items:

The set of packets that are allowed by the Checkpoint device, but denied by the Cisco device, are shown in the Policy Difference Table. There may be multiple tables, each caused by a specific problem. The remedy is the following:

1. The Checkpoint rule should not be removed or altered.
2. Add rules above this Checkpoint rule to deny each packet described in the Policy Difference Table below.
3. Use rule reduction techniques such as address aggregation, or object grouping to reduce the number of rules to be added

Policy Difference Table:

Policy Diff Item	Source	Destination	Service	Cisco Rule Trails
155	10.0.0.0/8	192.168.9.0/24	tcp/telnet	nat:nat/Default-Deny
168	172.16.0.0 to 172.16.0.23	192.168.9.0/24	tcp/telnet	nat:nat/Default-Deny
169	172.16.0.24	192.168.9.0/24	tcp/telnet	nat:nat/Default-Deny
187	172.17.0.0/16	192.168.9.0/24	tcp/telnet	nat:nat/Default-Deny
187	172.16.0.25 to 172.16.255.255	192.168.9.0/24	tcp/telnet	nat:nat/Default-Deny
193	192.168.5.0/24	192.168.9.0/24	tcp/telnet	nat:nat/Default-Deny
193	192.168.4.0/24	192.168.9.0/24	tcp/telnet	nat:nat/Default-Deny
193	192.168.3.0/24	192.168.9.0/24	tcp/telnet	nat:nat/Default-Deny
193	192.168.2.0/24	192.168.9.0/24	tcp/telnet	nat:nat/Default-Deny
220	10.0.0.0/8	192.168.1.0/24	tcp/telnet	nat:nat/Default-Deny
221	172.17.0.0/16	192.168.1.0/24	tcp/telnet	nat:nat/Default-Deny
222	192.168.5.0/24	192.168.1.0/24	tcp/telnet	nat:nat/Default-Deny
222	192.168.2.0/24	192.168.1.0/24	tcp/telnet	nat:nat/Default-Deny
222	192.168.4.0/24	192.168.1.0/24	tcp/telnet	nat:nat/Default-Deny
222	192.168.3.0/24	192.168.1.0/24	tcp/telnet	nat:nat/Default-Deny
267	192.168.4.0/24	192.168.50.0/24	tcp/telnet	nat:nat/Default-Deny
267	192.168.5.0/24	192.168.50.0/24	tcp/telnet	nat:nat/Default-Deny

Added policy caused by Checkpoint acl rule 10

Rule Index	Source	Destination	Service	VPN	Action	Comment
10	Host_172.16.0.68	Any	domain-udp		accept	(Original ACE (line 67): access-list acl_inside permit udp host 172.16.0.68 any eq domain)

Cisco Matching Rules:

Line No	Interface	Rule
67	inside	access-list acl_inside permit udp host 172.16.0.68 any eq domain

Difference caused by:

NAT control in Cisco Device

Problem Source:

NAT control in Cisco devices limits access to packets which are associated with NAT rules. Thus, the source, destination addresses, or services of allowed packets are smaller than what is indicated by this Checkpoint rule.

Remedy based on allow policies:

The set of packets that are allowed in the Cisco device are shown in the Allow Policy Table. To use this table:

1. Replace this Checkpoint rule with allow rules for packets described in each row of the table.
2. Use rule reduction techniques such as address aggregation, or object grouping to reduce the number of rules to be added.

Allow Policy Table:

Service	Source	Destination
udp/domain	172.16.0.68	0.0.0.0 to 9.255.255.255 11.0.0.0 to 172.15.255.255 172.18.0.0 to 192.168.1.255 192.168.6.0 to 192.168.8.255 192.168.10.0 to 255.255.255.255

Remedy based on policy diff items:

The set of packets that are allowed by the Checkpoint device, but denied by the Cisco device, are shown in the Policy Difference Table. There may be multiple tables, each caused by a specific problem. The remedy is the following:

1. The Checkpoint rule should not be removed or altered.
2. Add rules above this Checkpoint rule to deny each packet described in the Policy Difference Table below.
3. Use rule reduction techniques such as address aggregation, or object grouping to reduce the number of rules to be added

Policy Difference Table:

Policy Diff Item	Source	Destination	Service	Cisco Rule Trails
186	172.16.0.68	192.168.9.0/24	udp/domain	nat:nat/Default-Deny

Added policy caused by Checkpoint acl rule 11

Rule Index	Source	Destination	Service	VPN	Action	Comment
11	Migrated_inside_Interface	Any	tcp-9895		accept	(Original ACE (line 68): access-list acl_inside permit tcp any any eq 9895)

Cisco Overlap Rules:

Line No	Interface	Rule
	vpn4	high-to-low-default-allow
68	inside	access-list acl_inside permit tcp any any eq 9895

Difference caused by:

NAT control in Cisco Device

Problem Source:

NAT control in Cisco devices limits access to packets which are associated with NAT rules. Thus, the source, destination addresses, or services of allowed packets are smaller than what is indicated by this Checkpoint rule.

Remedy based on allow policies:

The set of packets that are allowed in the Cisco device are shown in the Allow Policy Table. To use this table:

1. Replace this Checkpoint rule with allow rules for packets described in each row of the table.
2. Use rule reduction techniques such as address aggregation, or object grouping to reduce the number of rules to be added.

Allow Policy Table:

Service	Source	Destination
tcp/9895	10.0.0.0/8	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 255.255.255.255
tcp/9895	172.16.0.0/15	0.0.0.0 to 9.255.255.255 11.0.0.0 to 172.15.255.255 192.168.6.0 to 192.168.8.255 192.168.10.0 to 255.255.255.255
tcp/9895	172.16.0.0/16	172.18.0.0 to 192.168.1.255
tcp/9895	172.17.0.0/16	172.18.0.0 to 192.168.0.255
tcp/9895	192.168.2.0 to 192.168.5.255	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
tcp/9895	192.168.2.0/23	192.168.10.0 to 255.255.255.255
tcp/9895	192.168.4.0/23	192.168.10.0 to 192.168.49.255 192.168.51.0 to 255.255.255.255

Remedy based on policy diff items:

The set of packets that are allowed by the Checkpoint device, but denied by the Cisco device, are shown in the Policy Difference Table. There may be multiple tables, each caused by a specific problem. The remedy is the following:

1. The Checkpoint rule should not be removed or altered.
2. Add rules above this Checkpoint rule to deny each packet described in the Policy Difference Table below.
3. Use rule reduction techniques such as address aggregation, or object grouping to reduce the number of rules to be added

Policy Difference Table:

Policy Diff Item	Source	Destination	Service	Cisco Rule Trails
165	10.0.0.0/8	192.168.9.0/24	tcp/9895	nat:nat/Default-Deny
185	172.16.0.0/15	192.168.9.0/24	tcp/9895	nat:nat/Default-Deny
203	192.168.2.0 to 192.168.5.255	192.168.9.0/24	tcp/9895	nat:nat/Default-Deny
250	10.0.0.0/8	192.168.1.0/24	tcp/9895	nat:nat/Default-Deny
251	172.17.0.0/16	192.168.1.0/24	tcp/9895	nat:nat/Default-Deny

Policy Diff Item	Source	Destination	Service	Cisco Rule Trails
252	192.168.2.0 to 192.168.5.255	192.168.1.0/24	tcp/9895	nat:nat/Default-Deny
279	192.168.4.0/23	192.168.50.0/24	tcp/9895	nat:nat/Default-Deny

Added policy caused by Checkpoint acl rule 12

Rule Index	Source	Destination	Service	VPN	Action	Comment
12	Migrated_inside_Interface	Any	nntp		accept	(Original ACE (line 69): access-list acl_inside permit tcp any any eq nntp)

Cisco Overlap Rules:

Line No	Interface	Rule
	vpn4	high-to-low-default-allow
69	inside	access-list acl_inside permit tcp any any eq nntp
88	inside	access-list acl_inside permit tcp 172.16.0.0 255.255.0.0 any eq nntp

Difference caused by:

NAT control in Cisco Device

Problem Source:

NAT control in Cisco devices limits access to packets which are associated with NAT rules. Thus, the source, destination addresses, or services of allowed packets are smaller than what is indicated by this Checkpoint rule.

Remedy based on allow policies:

The set of packets that are allowed in the Cisco device are shown in the Allow Policy Table. To use this table:

1. Replace this Checkpoint rule with allow rules for packets described in each row of the table.
2. Use rule reduction techniques such as address aggregation, or object grouping to reduce the number of rules to be added.

Allow Policy Table:

Service	Source	Destination
tcp/nntp	10.0.0.0/8	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 255.255.255.255
tcp/nntp	172.16.0.0/15	0.0.0.0 to 9.255.255.255 11.0.0.0 to 172.15.255.255 192.168.6.0 to 192.168.8.255 192.168.10.0 to 255.255.255.255
tcp/nntp	172.16.0.0/16	172.18.0.0 to 192.168.1.255

Service	Source	Destination
tcp/nntp	172.17.0.0/16	172.18.0.0 to 192.168.0.255
tcp/nntp	192.168.2.0 to 192.168.5.255	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
tcp/nntp	192.168.2.0/23	192.168.10.0 to 255.255.255.255
tcp/nntp	192.168.4.0/23	192.168.10.0 to 192.168.49.255 192.168.51.0 to 255.255.255.255

Remedy based on policy diff items:

The set of packets that are allowed by the Checkpoint device, but denied by the Cisco device, are shown in the Policy Difference Table. There may be multiple tables, each caused by a specific problem. The remedy is the following:

1. The Checkpoint rule should not be removed or altered.
2. Add rules above this Checkpoint rule to deny each packet described in the Policy Difference Table below.
3. Use rule reduction techniques such as address aggregation, or object grouping to reduce the number of rules to be added

Policy Difference Table:

Policy Diff Item	Source	Destination	Service	Cisco Rule Trails
157	10.0.0.0/8	192.168.9.0/24	tcp/nntp	nat:nat/Default-Deny
177	172.16.0.0/15	192.168.9.0/24	tcp/nntp	nat:nat/Default-Deny
195	192.168.2.0 to 192.168.5.255	192.168.9.0/24	tcp/nntp	nat:nat/Default-Deny
226	10.0.0.0/8	192.168.1.0/24	tcp/nntp	nat:nat/Default-Deny
227	172.17.0.0/16	192.168.1.0/24	tcp/nntp	nat:nat/Default-Deny
228	192.168.2.0 to 192.168.5.255	192.168.1.0/24	tcp/nntp	nat:nat/Default-Deny
269	192.168.4.0/23	192.168.50.0/24	tcp/nntp	nat:nat/Default-Deny

Added policy caused by Checkpoint acl rule 13

Rule Index	Source	Destination	Service	VPN	Action	Comment
13	Host_172.16.0.68	Any	nntp-udp		accept	(Original ACE (line 70): access-list acl_inside permit udp host 172.16.0.68 any eq nntp)

Cisco Matching Rules:

Line No	Interface	Rule
70	inside	access-list acl_inside permit udp host 172.16.0.68 any eq nntp

Difference caused by:

NAT control in Cisco Device

Problem Source:

NAT control in Cisco devices limits access to packets which are associated with NAT rules. Thus, the source, destination addresses, or services of allowed packets are smaller than what is indicated by this Checkpoint rule.

Remedy based on allow policies:

The set of packets that are allowed in the Cisco device are shown in the Allow Policy Table. To use this table:

1. Replace this Checkpoint rule with allow rules for packets described in each row of the table.
2. Use rule reduction techniques such as address aggregation, or object grouping to reduce the number of rules to be added.

Allow Policy Table:

Service	Source	Destination
udp/ntp	172.16.0.68	0.0.0.0 to 9.255.255.255 11.0.0.0 to 172.15.255.255 172.18.0.0 to 192.168.1.255 192.168.6.0 to 192.168.8.255 192.168.10.0 to 255.255.255.255

Remedy based on policy diff items:

The set of packets that are allowed by the Checkpoint device, but denied by the Cisco device, are shown in the Policy Difference Table. There may be multiple tables, each caused by a specific problem. The remedy is the following:

1. The Checkpoint rule should not be removed or altered.
2. Add rules above this Checkpoint rule to deny each packet described in the Policy Difference Table below.
3. Use rule reduction techniques such as address aggregation, or object grouping to reduce the number of rules to be added

Policy Difference Table:

Policy Diff Item	Source	Destination	Service	Cisco Rule Trails
186	172.16.0.68	192.168.9.0/24	udp/ntp	nat:nat/Default-Deny

Added policy caused by Checkpoint acl rule 14

Rule Index	Source	Destination	Service	VPN	Action	Comment
14	Host_172.16.0.25	Any	aimpp-port-req		accept	(Original ACE (line 71): access-list acl_inside permit tcp host 172.16.0.25 any eq 2847)

Cisco Matching Rules:

Line No	Interface	Rule
71	inside	access-list acl_inside permit tcp host 172.16.0.25 any eq 2847

Difference caused by:

NAT control in Cisco Device

Problem Source:

NAT control in Cisco devices limits access to packets which are associated with NAT rules. Thus, the source, destination addresses, or services of allowed packets are smaller than what is indicated by this Checkpoint rule.

Remedy based on allow policies:

The set of packets that are allowed in the Cisco device are shown in the Allow Policy Table. To use this table:

1. Replace this Checkpoint rule with allow rules for packets described in each row of the table.
2. Use rule reduction techniques such as address aggregation, or object grouping to reduce the number of rules to be added.

Allow Policy Table:

Service	Source	Destination
tcp/aimpp-port-req	172.16.0.25	0.0.0.0 to 9.255.255.255 11.0.0.0 to 172.15.255.255 172.18.0.0 to 192.168.1.255 192.168.6.0 to 192.168.8.255 192.168.10.0 to 255.255.255.255

Remedy based on policy diff items:

The set of packets that are allowed by the Checkpoint device, but denied by the Cisco device, are shown in the Policy Difference Table. There may be multiple tables, each caused by a specific problem. The remedy is the following:

1. The Checkpoint rule should not be removed or altered.
2. Add rules above this Checkpoint rule to deny each packet described in the Policy Difference Table below.
3. Use rule reduction techniques such as address aggregation, or object grouping to reduce the number of rules to be added

Policy Difference Table:

Policy Diff Item	Source	Destination	Service	Cisco Rule Trails
170	172.16.0.25	192.168.9.0/24	tcp/aimpp-port-req	nat:nat/Default-Deny

Added policy caused by Checkpoint acl rule 15

Rule Index	Source	Destination	Service	VPN	Action	Comment
15	Host_172.16.0.25	Any	tcp-amt-blc-port		accept	(Original ACE (line 72): access-list acl_inside permit tcp host 172.16.0.25 any eq 2848)

Cisco Matching Rules:

Line No	Interface	Rule
72	inside	access-list acl_inside permit tcp host 172.16.0.25 any eq 2848

Difference caused by:

NAT control in Cisco Device

Problem Source:

NAT control in Cisco devices limits access to packets which are associated with NAT rules. Thus, the source, destination addresses, or services of allowed packets are smaller than what is indicated by this Checkpoint rule.

Remedy based on allow policies:

The set of packets that are allowed in the Cisco device are shown in the Allow Policy Table. To use this table:

1. Replace this Checkpoint rule with allow rules for packets described in each row of the table.
2. Use rule reduction techniques such as address aggregation, or object grouping to reduce the number of rules to be added.

Allow Policy Table:

Service	Source	Destination
tcp/amt-blc-port	172.16.0.25	0.0.0.0 to 9.255.255.255 11.0.0.0 to 172.15.255.255 172.18.0.0 to 192.168.1.255 192.168.6.0 to 192.168.8.255 192.168.10.0 to 255.255.255.255

Remedy based on policy diff items:

The set of packets that are allowed by the Checkpoint device, but denied by the Cisco device, are shown in the Policy Difference Table. There may be multiple tables, each caused by a specific problem. The remedy is the following:

1. The Checkpoint rule should not be removed or altered.
2. Add rules above this Checkpoint rule to deny each packet described in the Policy Difference Table below.
3. Use rule reduction techniques such as address aggregation, or object grouping to reduce the number of rules to be added

Policy Difference Table:

Policy Diff Item	Source	Destination	Service	Cisco Rule Trails
170	172.16.0.25	192.168.9.0/24	tcp/amt-blc-port	nat:nat/Default-Deny

Added policy caused by Checkpoint acl rule 16

Rule Index	Source	Destination	Service	VPN	Action	Comment
16	Migrated_inside_Interface	Any	tcp-7618		accept	(Original ACE (line 73): access-list acl_inside permit tcp any any eq 7618)

Cisco Overlap Rules:

Line No	Interface	Rule
	vpn4	high-to-low-default-allow
73	inside	access-list acl_inside permit tcp any any eq 7618

Difference caused by:

NAT control in Cisco Device

Problem Source:

NAT control in Cisco devices limits access to packets which are associated with NAT rules. Thus, the source, destination addresses, or services of allowed packets are smaller than what is indicated by this Checkpoint rule.

Remedy based on allow policies:

The set of packets that are allowed in the Cisco device are shown in the Allow Policy Table. To use this table:

1. Replace this Checkpoint rule with allow rules for packets described in each row of the table.
2. Use rule reduction techniques such as address aggregation, or object grouping to reduce the number of rules to be added.

Allow Policy Table:

Service	Source	Destination
---------	--------	-------------

Service	Source	Destination
tcp/7618	10.0.0.0/8	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 255.255.255.255
tcp/7618	172.16.0.0/15	0.0.0.0 to 9.255.255.255 11.0.0.0 to 172.15.255.255 192.168.6.0 to 192.168.8.255 192.168.10.0 to 255.255.255.255
tcp/7618	172.16.0.0/16	172.18.0.0 to 192.168.1.255
tcp/7618	172.17.0.0/16	172.18.0.0 to 192.168.0.255
tcp/7618	192.168.2.0 to 192.168.5.255	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
tcp/7618	192.168.2.0/23	192.168.10.0 to 255.255.255.255
tcp/7618	192.168.4.0/23	192.168.10.0 to 192.168.49.255 192.168.51.0 to 255.255.255.255

Remedy based on policy diff items:

The set of packets that are allowed by the Checkpoint device, but denied by the Cisco device, are shown in the Policy Difference Table. There may be multiple tables, each caused by a specific problem. The remedy is the following:

1. The Checkpoint rule should not be removed or altered.
2. Add rules above this Checkpoint rule to deny each packet described in the Policy Difference Table below.
3. Use rule reduction techniques such as address aggregation, or object grouping to reduce the number of rules to be added

Policy Difference Table:

Policy Diff Item	Source	Destination	Service	Cisco Rule Trails
162	10.0.0.0/8	192.168.9.0/24	tcp/7618	nat:nat/Default-Deny
182	172.16.0.0/15	192.168.9.0/24	tcp/7618	nat:nat/Default-Deny
200	192.168.2.0 to 192.168.5.255	192.168.9.0/24	tcp/7618	nat:nat/Default-Deny
241	10.0.0.0/8	192.168.1.0/24	tcp/7618	nat:nat/Default-Deny
242	172.17.0.0/16	192.168.1.0/24	tcp/7618	nat:nat/Default-Deny
243	192.168.2.0 to 192.168.5.255	192.168.1.0/24	tcp/7618	nat:nat/Default-Deny
276	192.168.4.0/23	192.168.50.0/24	tcp/7618	nat:nat/Default-Deny

Added policy caused by Checkpoint acl rule 17

Rule Index	Source	Destination	Service	VPN	Action	Comment
17	Migrated_inside_Interface	Any	http-halt		accept	(Original ACE (line 74): access-list acl_inside permit tcp any any eq 8080)

Cisco Overlap Rules:

Line No	Interface	Rule
	vpn4	high-to-low-default-allow
74	inside	access-list acl_inside permit tcp any any eq 8080

Difference caused by:

NAT control in Cisco Device

Problem Source:

NAT control in Cisco devices limits access to packets which are associated with NAT rules. Thus, the source, destination addresses, or services of allowed packets are smaller than what is indicated by this Checkpoint rule.

Remedy based on allow policies:

The set of packets that are allowed in the Cisco device are shown in the Allow Policy Table. To use this table:

1. Replace this Checkpoint rule with allow rules for packets described in each row of the table.
2. Use rule reduction techniques such as address aggregation, or object grouping to reduce the number of rules to be added.

Allow Policy Table:

Service	Source	Destination
tcp/http-alt	10.0.0.0/8	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 255.255.255.255
tcp/http-alt	172.16.0.0/15	0.0.0.0 to 9.255.255.255 11.0.0.0 to 172.15.255.255 192.168.6.0 to 192.168.8.255 192.168.10.0 to 255.255.255.255
tcp/http-alt	172.16.0.0/16	172.18.0.0 to 192.168.1.255
tcp/http-alt	172.17.0.0/16	172.18.0.0 to 192.168.0.255
tcp/http-alt	192.168.2.0 to 192.168.5.255	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
tcp/http-alt	192.168.2.0/23	192.168.10.0 to 255.255.255.255
tcp/http-alt	192.168.4.0/23	192.168.10.0 to 192.168.49.255 192.168.51.0 to 255.255.255.255

Remedy based on policy diff items:

The set of packets that are allowed by the Checkpoint device, but denied by the Cisco device, are shown in the Policy Difference Table. There may be multiple tables, each caused by a specific problem. The remedy is the following:

1. The Checkpoint rule should not be removed or altered.
2. Add rules above this Checkpoint rule to deny each packet described in the Policy Difference Table below.
3. Use rule reduction techniques such as address aggregation, or object grouping to reduce the number of rules to be added

Policy Difference Table:

Policy Diff Item	Source	Destination	Service	Cisco Rule Trails
164	10.0.0.0/8	192.168.9.0/24	tcp/http-alt	nat:nat/Default-Deny
184	172.16.0.0/15	192.168.9.0/24	tcp/http-alt	nat:nat/Default-Deny
202	192.168.2.0 to 192.168.5.255	192.168.9.0/24	tcp/http-alt	nat:nat/Default-Deny
247	10.0.0.0/8	192.168.1.0/24	tcp/http-alt	nat:nat/Default-Deny
248	172.17.0.0/16	192.168.1.0/24	tcp/http-alt	nat:nat/Default-Deny
249	192.168.2.0 to 192.168.5.255	192.168.1.0/24	tcp/http-alt	nat:nat/Default-Deny
278	192.168.4.0/23	192.168.50.0/24	tcp/http-alt	nat:nat/Default-Deny

Added policy caused by Checkpoint acl rule 18

Rule Index	Source	Destination	Service	VPN	Action	Comment
18	Host_172.16.0.19	Any	smtp		accept	(Original ACE (line 75): access-list acl_inside permit tcp host 172.16.0.19 any eq smtp)

Cisco Matching Rules:

Line No	Interface	Rule
75	inside	access-list acl_inside permit tcp host 172.16.0.19 any eq smtp

Difference caused by:

NAT control in Cisco Device

Problem Source:

NAT control in Cisco devices limits access to packets which are associated with NAT rules. Thus, the source, destination addresses, or services of allowed packets are smaller than what is indicated by this Checkpoint rule.

Remedy based on allow policies:

The set of packets that are allowed in the Cisco device are shown in the Allow Policy Table. To use this table:

1. Replace this Checkpoint rule with allow rules for packets described in each row of the table.
2. Use rule reduction techniques such as address aggregation, or object grouping to reduce the number of rules to be added.

Allow Policy Table:

Service	Source	Destination
tcp/smtp	172.16.0.19	0.0.0.0 to 9.255.255.255 11.0.0.0 to 172.15.255.255 172.18.0.0 to 192.168.1.255 192.168.6.0 to 192.168.8.255 192.168.10.0 to 255.255.255.255

Remedy based on policy diff items:

The set of packets that are allowed by the Checkpoint device, but denied by the Cisco device, are shown in the Policy Difference Table. There may be multiple tables, each caused by a specific problem. The remedy is the following:

1. The Checkpoint rule should not be removed or altered.
2. Add rules above this Checkpoint rule to deny each packet described in the Policy Difference Table below.
3. Use rule reduction techniques such as address aggregation, or object grouping to reduce the number of rules to be added

Policy Difference Table:

Policy Diff Item	Source	Destination	Service	Cisco Rule Trails
167	172.16.0.19	192.168.9.0/24	tcp/smtp	nat:nat/Default-Deny

Added policy caused by Checkpoint acl rule 21

Rule Index	Source	Destination	Service	VPN	Action	Comment
21	Migrated_inside_Interface	Any	Migrated_sjpix_ICMP_Any		accept	(Original ACE (line 78): access-list acl_inside permit icmp any any)

Cisco Overlap Rules:

Line No	Interface	Rule
	vpn4	high-to-low-default-allow
107	testweb	access-list acl_testweb permit icmp any any
111	proxymail	access-list acl_proxymail permit icmp any any
50	outside	access-list acl_outside permit icmp any host 62.59.14.169
78	inside	access-list acl_inside permit icmp any any

Difference caused by:

NAT control in Cisco Device

Problem Source:

NAT control in Cisco devices limits access to packets which are associated with NAT rules. Thus, the source, destination addresses, or services of allowed packets are smaller than what is indicated by this Checkpoint rule.

Remedy based on allow policies:

The set of packets that are allowed in the Cisco device are shown in the Allow Policy Table. To use this table:

1. Replace this Checkpoint rule with allow rules for packets described in each row of the table.
2. Use rule reduction techniques such as address aggregation, or object grouping to reduce the number of rules to be added.

Allow Policy Table:

Service	Source	Destination
icmp	10.0.0.0/8	0.0.0.0 to 9.255.255.255 11.0.0.0 to 172.15.255.255 172.16.0.1 172.18.0.0 to 192.168.0.255 192.168.6.0 to 192.168.8.255 192.168.10.0 to 255.255.255.255
icmp	172.16.0.0	0.0.0.0 to 9.255.255.255 11.0.0.0 to 172.15.255.255 172.16.0.1 172.18.0.0 to 192.168.1.255 192.168.6.0 to 192.168.8.255
icmp	172.16.0.1	0.0.0.0 to 192.168.8.255
icmp	172.16.0.2 to 172.17.255.255	0.0.0.0 to 9.255.255.255 11.0.0.0 to 172.15.255.255 172.16.0.1 192.168.6.0 to 192.168.8.255
icmp	172.16.0.2 to 172.16.255.255	172.18.0.0 to 192.168.1.255
icmp	172.17.0.0/16	172.18.0.0 to 192.168.0.255
icmp	192.168.2.0 to 192.168.5.255	0.0.0.0 to 9.255.255.255 11.0.0.0 to 172.15.255.255 172.16.0.1 172.18.0.0 to 192.168.0.255 192.168.6.0 to 192.168.8.255
icmp	172.16.0.0/15 192.168.2.0/23	192.168.10.0 to 255.255.255.255
icmp	192.168.4.0/23	192.168.10.0 to 192.168.49.255 192.168.51.0 to 255.255.255.255

Remedy based on policy diff items:

The set of packets that are allowed by the Checkpoint device, but denied by the Cisco device, are shown in the Policy Difference Table. There may be multiple tables, each caused by a specific problem. The remedy is the following:

1. The Checkpoint rule should not be removed or altered.
2. Add rules above this Checkpoint rule to deny each packet described in the Policy Difference Table below.
3. Use rule reduction techniques such as address aggregation, or object grouping to reduce the number of rules to be added

Policy Difference Table:

Policy Diff Item	Source	Destination	Service	Cisco Rule Trails
150	10.0.0.0/8	192.168.9.0/24	icmp	nat:nat/Default-Deny
171	172.16.0.0/15	192.168.9.0/24	icmp	nat:nat/Default-Deny
188	192.168.2.0 to 192.168.5.255	192.168.9.0/24	icmp	nat:nat/Default-Deny
205	10.0.0.0/8	192.168.1.0/24	icmp	nat:nat/Default-Deny
210	172.17.0.0/16	192.168.1.0/24	icmp	nat:nat/Default-Deny
215	192.168.2.0 to 192.168.5.255	192.168.1.0/24	icmp	nat:nat/Default-Deny
262	192.168.4.0/23	192.168.50.0/24	icmp	nat:nat/Default-Deny

Added policy caused by Checkpoint acl rule 22

Rule Index	Source	Destination	Service	VPN	Action	Comment
22	Migrated_inside_Interface	Any	H323		accept	(Original ACE (line 79): access-list acl_inside permit tcp any any eq h323)

Cisco Overlap Rules:

Line No	Interface	Rule
	vpn4	high-to-low-default-allow

Difference caused by:

ACL rules with allow action and "any" only in destination

Problem Source:

Device architecture difference allows more packets in the Checkpoint device than the equivalent rule in the Cisco device. Another cause may be the absence of an equivalent Cisco rule.

Remedy:

Add deny rules in front of this Checkpoint rule to deny the policy items listed below.

Remedy based on policy diff items:

The set of packets that are allowed by the Checkpoint device, but denied by the Cisco device, are shown in the Policy Difference Table. There may be multiple tables, each caused by a specific problem. The remedy is the following:

1. The Checkpoint rule should not be removed or altered.
2. Add rules above this Checkpoint rule to deny each packet described in the Policy Difference Table below.

3. Use rule reduction techniques such as address aggregation, or object grouping to reduce the number of rules to be added.

Policy Difference Table:

Policy Diff Item	Source	Destination	Service	Cisco Rule Trails
159	10.0.0.0/8	192.168.9.0/24	tcp/h323hostcall	acl:access-list-acl_inside- implied-deny
179	172.16.0.0/15	192.168.9.0/24	tcp/h323hostcall	acl:access-list-acl_inside- implied-deny
197	192.168.2.0 to 192.168.5.255	192.168.9.0/24	tcp/h323hostcall	acl:access-list-acl_inside- implied-deny
232	10.0.0.0/8	192.168.1.0/24	tcp/h323hostcall	acl:access-list-acl_inside- implied-deny
233	172.16.0.0/15	192.168.1.0/24	tcp/h323hostcall	acl:access-list-acl_inside- implied-deny
234	192.168.2.0 to 192.168.5.255	192.168.1.0/24	tcp/h323hostcall	acl:access-list-acl_inside- implied-deny
271	10.0.0.0/8	192.168.50.0/24	tcp/h323hostcall	acl:access-list-acl_inside- implied-deny
272	172.16.0.0/15	192.168.50.0/24	tcp/h323hostcall	acl:access-list-acl_inside- implied-deny
273	192.168.2.0 to 192.168.5.255	192.168.50.0/24	tcp/h323hostcall	acl:access-list-acl_inside- implied-deny
299	10.0.0.0/8	0.0.0.0 to 9.255.255.255	tcp/h323hostcall	acl:access-list-acl_inside- implied-deny
300	10.0.0.0/8	11.0.0.0 to 172.15.255.255	tcp/h323hostcall	acl:access-list-acl_inside- implied-deny
301	10.0.0.0/8	172.18.0.0 to 192.168.0.255	tcp/h323hostcall	acl:access-list-acl_inside- implied-deny
302	10.0.0.0/8	192.168.6.0 to 192.168.8.255	tcp/h323hostcall	acl:access-list-acl_inside- implied-deny
303	10.0.0.0/8	192.168.10.0 to 192.168.49.255	tcp/h323hostcall	acl:access-list-acl_inside- implied-deny
304	10.0.0.0/8	192.168.51.0 to 255.255.255.255	tcp/h323hostcall	acl:access-list-acl_inside- implied-deny
305	172.16.0.0/15	0.0.0.0 to 9.255.255.255	tcp/h323hostcall	acl:access-list-acl_inside- implied-deny
306	172.16.0.0/15	11.0.0.0 to 172.15.255.255	tcp/h323hostcall	acl:access-list-acl_inside- implied-deny
307	172.16.0.0/15	172.18.0.0 to 192.168.0.255	tcp/h323hostcall	acl:access-list-acl_inside- implied-deny
308	172.16.0.0/15	192.168.6.0 to 192.168.8.255	tcp/h323hostcall	acl:access-list-acl_inside- implied-deny
309	172.16.0.0/15	192.168.10.0 to 192.168.49.255	tcp/h323hostcall	acl:access-list-acl_inside- implied-deny
310	172.16.0.0/15	192.168.51.0 to 255.255.255.255	tcp/h323hostcall	acl:access-list-acl_inside- implied-deny
311	192.168.2.0 to 192.168.5.255	0.0.0.0 to 9.255.255.255	tcp/h323hostcall	acl:access-list-acl_inside- implied-deny
312	192.168.2.0 to 192.168.5.255	11.0.0.0 to 172.15.255.255	tcp/h323hostcall	acl:access-list-acl_inside- implied-deny
313	192.168.2.0 to 192.168.5.255	172.18.0.0 to 192.168.0.255	tcp/h323hostcall	acl:access-list-acl_inside- implied-deny
314	192.168.2.0 to 192.168.5.255	192.168.6.0 to 192.168.8.255	tcp/h323hostcall	acl:access-list-acl_inside- implied-deny
315	192.168.2.0 to 192.168.5.255	192.168.10.0 to 192.168.49.255	tcp/h323hostcall	acl:access-list-acl_inside- implied-deny
316	192.168.2.0 to 192.168.5.255	192.168.51.0 to 255.255.255.255	tcp/h323hostcall	acl:access-list-acl_inside- implied-deny

Added policy caused by Checkpoint acl rule 23

Rule Index	Source	Destination	Service	VPN	Action	Comment
23	Host_192.168.5.251	Any	all_udp		accept	(Original ACE (line 80): access-list acl_inside permit udp host 192.168.5.251 any)

Cisco Matching Rules:

Line No	Interface	Rule
80	inside	access-list acl_inside permit udp host 192.168.5.251 any

Difference caused by:

NAT control in Cisco Device

Problem Source:

NAT control in Cisco devices limits access to packets which are associated with NAT rules. Thus, the source, destination addresses, or services of allowed packets are smaller than what is indicated by this Checkpoint rule.

Remedy based on allow policies:

The set of packets that are allowed in the Cisco device are shown in the Allow Policy Table. To use this table:

1. Replace this Checkpoint rule with allow rules for packets described in each row of the table.
2. Use rule reduction techniques such as address aggregation, or object grouping to reduce the number of rules to be added.

Allow Policy Table:

Service	Source	Destination
udp/any	192.168.5.251	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

Remedy based on policy diff items:

The set of packets that are allowed by the Checkpoint device, but denied by the Cisco device, are shown in the Policy Difference Table. There may be multiple tables, each caused by a specific problem. The remedy is the following:

1. The Checkpoint rule should not be removed or altered.
2. Add rules above this Checkpoint rule to deny each packet described in the Policy Difference Table below.
3. Use rule reduction techniques such as address aggregation, or object grouping to reduce the number of rules to be added

Policy Difference Table:

Policy Diff Item	Source	Destination	Service	Cisco Rule Trails
204	192.168.5.251	192.168.9.0/24	udp/any	nat:nat/Default-Deny
255	192.168.5.251	192.168.1.0/24	udp/any	nat:nat/Default-Deny
280	192.168.5.251	192.168.50.0/24	udp/any	nat:nat/Default-Deny

Added policy caused by Checkpoint acl rule 24

Rule Index	Source	Destination	Service	VPN	Action	Comment
24	Migrated_inside_Interface	Any	tcp-5900		accept	(Original ACE (line 81): access-list acl_inside permit tcp any any eq 5900)

Cisco Overlap Rules:

Line No	Interface	Rule
	vpn4	high-to-low-default-allow
81	inside	access-list acl_inside permit tcp any any eq 5900

Difference caused by:

NAT control in Cisco Device

Problem Source:

NAT control in Cisco devices limits access to packets which are associated with NAT rules. Thus, the source, destination addresses, or services of allowed packets are smaller than what is indicated by this Checkpoint rule.

Remedy based on allow policies:

The set of packets that are allowed in the Cisco device are shown in the Allow Policy Table. To use this table:

1. Replace this Checkpoint rule with allow rules for packets described in each row of the table.
2. Use rule reduction techniques such as address aggregation, or object grouping to reduce the number of rules to be added.

Allow Policy Table:

Service	Source	Destination
tcp/vnc-server	10.0.0.0/8	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 255.255.255.255

Service	Source	Destination
tcp/vnc-server	172.16.0.0/15	0.0.0.0 to 9.255.255.255 11.0.0.0 to 172.15.255.255 192.168.6.0 to 192.168.8.255 192.168.10.0 to 255.255.255.255
tcp/vnc-server	172.16.0.0/16	172.18.0.0 to 192.168.1.255
tcp/vnc-server	172.17.0.0/16	172.18.0.0 to 192.168.0.255
tcp/vnc-server	192.168.2.0 to 192.168.5.255	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
tcp/vnc-server	192.168.2.0/23	192.168.10.0 to 255.255.255.255
tcp/vnc-server	192.168.4.0/23	192.168.10.0 to 192.168.49.255 192.168.51.0 to 255.255.255.255

Remedy based on policy diff items:

The set of packets that are allowed by the Checkpoint device, but denied by the Cisco device, are shown in the Policy Difference Table. There may be multiple tables, each caused by a specific problem. The remedy is the following:

1. The Checkpoint rule should not be removed or altered.
2. Add rules above this Checkpoint rule to deny each packet described in the Policy Difference Table below.
3. Use rule reduction techniques such as address aggregation, or object grouping to reduce the number of rules to be added

Policy Difference Table:

Policy Diff Item	Source	Destination	Service	Cisco Rule Trails
161	10.0.0.0/8	192.168.9.0/24	tcp/vnc-server	nat:nat/Default-Deny
181	172.17.0.0/16	192.168.9.0/24	tcp/vnc-server	nat:nat/Default-Deny
181	172.16.0.0/16	192.168.9.0/24	tcp/vnc-server	nat:nat/Default-Deny
199	192.168.4.0/24	192.168.9.0/24	tcp/vnc-server	nat:nat/Default-Deny
199	192.168.3.0/24	192.168.9.0/24	tcp/vnc-server	nat:nat/Default-Deny
199	192.168.5.0/24	192.168.9.0/24	tcp/vnc-server	nat:nat/Default-Deny
199	192.168.2.0/24	192.168.9.0/24	tcp/vnc-server	nat:nat/Default-Deny
238	10.0.0.0/8	192.168.1.0/24	tcp/vnc-server	nat:nat/Default-Deny
239	172.17.0.0/16	192.168.1.0/24	tcp/vnc-server	nat:nat/Default-Deny
240	192.168.5.0/24	192.168.1.0/24	tcp/vnc-server	nat:nat/Default-Deny
240	192.168.2.0/24	192.168.1.0/24	tcp/vnc-server	nat:nat/Default-Deny
240	192.168.3.0/24	192.168.1.0/24	tcp/vnc-server	nat:nat/Default-Deny
240	192.168.4.0/24	192.168.1.0/24	tcp/vnc-server	nat:nat/Default-Deny
275	192.168.5.0/24	192.168.50.0/24	tcp/vnc-server	nat:nat/Default-Deny
275	192.168.4.0/24	192.168.50.0/24	tcp/vnc-server	nat:nat/Default-Deny

Added policy caused by Checkpoint acl rule 25

Rule Index	Source	Destination	Service	VPN	Action	Comment
25	Migrated_Host_Plain_192.168.5.250	Any	all_udp		accept	(Original ACE (line 82): access-list acl_inside permit udp host 192.168.5.250 any)

Cisco Matching Rules:

Line No	Interface	Rule
82	inside	access-list acl_inside permit udp host 192.168.5.250 any

Difference caused by:

NAT control in Cisco Device

Problem Source:

NAT control in Cisco devices limits access to packets which are associated with NAT rules. Thus, the source, destination addresses, or services of allowed packets are smaller than what is indicated by this Checkpoint rule.

Remedy based on allow policies:

The set of packets that are allowed in the Cisco device are shown in the Allow Policy Table. To use this table:

1. Replace this Checkpoint rule with allow rules for packets described in each row of the table.
2. Use rule reduction techniques such as address aggregation, or object grouping to reduce the number of rules to be added.

Allow Policy Table:

Service	Source	Destination
udp/any	192.168.5.250	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

Remedy based on policy diff items:

The set of packets that are allowed by the Checkpoint device, but denied by the Cisco device, are shown in the Policy Difference Table. There may be multiple tables, each caused by a specific problem. The remedy is the following:

1. The Checkpoint rule should not be removed or altered.
2. Add rules above this Checkpoint rule to deny each packet described in the Policy Difference Table below.
3. Use rule reduction techniques such as address aggregation, or object grouping to reduce the number of rules to be added

Policy Difference Table:

Policy Diff Item	Source	Destination	Service	Cisco Rule Trails
204	192.168.5.250	192.168.9.0/24	udp/any	nat:nat/Default-Deny
255	192.168.5.250	192.168.1.0/24	udp/any	nat:nat/Default-Deny
280	192.168.5.250	192.168.50.0/24	udp/any	nat:nat/Default-Deny

Added policy caused by Checkpoint acl rule 26

Rule Index	Source	Destination	Service	VPN	Action	Comment
26	Migrated_inside_Interface	Host_192.168.50.2	tcp-5901		accept	(Original ACE (line 83): access-list acl_inside permit tcp any host 192.168.50.2 eq 5901)

Cisco Overlap Rules:

Line No	Interface	Rule
	vpn4	high-to-low-default-allow
83	inside	access-list acl_inside permit tcp any host 192.168.50.2 eq 5901
84	inside	access-list acl_inside permit tcp any any eq 5901

Difference caused by:

NAT control in Cisco Device

Problem Source:

NAT control in Cisco devices limits access to packets which are associated with NAT rules. Thus, the source, destination addresses, or services of allowed packets are smaller than what is indicated by this Checkpoint rule.

Remedy based on allow policies:

The set of packets that are allowed in the Cisco device are shown in the Allow Policy Table. To use this table:

1. Replace this Checkpoint rule with allow rules for packets described in each row of the table.
2. Use rule reduction techniques such as address aggregation, or object grouping to reduce the number of rules to be added.

Allow Policy Table:

Service	Source	Destination
tcp/5901	10.0.0.0/8 172.16.0.0/15	192.168.50.2

Service	Source	Destination
tcp/5901	192.168.2.0/23	192.168.50.2

Remedy based on policy diff items:

The set of packets that are allowed by the Checkpoint device, but denied by the Cisco device, are shown in the Policy Difference Table. There may be multiple tables, each caused by a specific problem. The remedy is the following:

1. The Checkpoint rule should not be removed or altered.
2. Add rules above this Checkpoint rule to deny each packet described in the Policy Difference Table below.
3. Use rule reduction techniques such as address aggregation, or object grouping to reduce the number of rules to be added

Policy Difference Table:

Policy Diff Item	Source	Destination	Service	Cisco Rule Trails
275	192.168.4.0/24	192.168.50.2	tcp/5901	nat:nat/Default-Deny
275	192.168.5.0/24	192.168.50.2	tcp/5901	nat:nat/Default-Deny

Added policy caused by Checkpoint acl rule 27

Rule Index	Source	Destination	Service	VPN	Action	Comment
27	Migrated_inside_Interface	Any	tcp-5901		accept	(Original ACE (line 84): access-list acl_inside permit tcp any any eq 5901)

Cisco Overlap Rules:

Line No	Interface	Rule
	vpn4	high-to-low-default-allow
83	inside	access-list acl_inside permit tcp any host 192.168.50.2 eq 5901
84	inside	access-list acl_inside permit tcp any any eq 5901

Difference caused by:

NAT control in Cisco Device

Problem Source:

NAT control in Cisco devices limits access to packets which are associated with NAT rules. Thus, the source, destination addresses, or services of allowed packets are smaller than what is indicated by this Checkpoint rule.

Remedy based on allow policies:

The set of packets that are allowed in the Cisco device are shown in the Allow Policy Table. To use this table:

1. Replace this Checkpoint rule with allow rules for packets described in each row of the table.
2. Use rule reduction techniques such as address aggregation, or object grouping to reduce the number of rules to be added.

Allow Policy Table:

Service	Source	Destination
tcp/5901	10.0.0.0/8	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 255.255.255.255
tcp/5901	172.16.0.0/15	0.0.0.0 to 9.255.255.255 11.0.0.0 to 172.15.255.255 192.168.6.0 to 192.168.8.255 192.168.10.0 to 255.255.255.255
tcp/5901	172.16.0.0/16	172.18.0.0 to 192.168.1.255
tcp/5901	172.17.0.0/16	172.18.0.0 to 192.168.0.255
tcp/5901	192.168.2.0 to 192.168.5.255	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
tcp/5901	192.168.2.0/23	192.168.10.0 to 255.255.255.255
tcp/5901	192.168.4.0/23	192.168.10.0 to 192.168.49.255 192.168.51.0 to 255.255.255.255

Remedy based on policy diff items:

The set of packets that are allowed by the Checkpoint device, but denied by the Cisco device, are shown in the Policy Difference Table. There may be multiple tables, each caused by a specific problem. The remedy is the following:

1. The Checkpoint rule should not be removed or altered.
2. Add rules above this Checkpoint rule to deny each packet described in the Policy Difference Table below.
3. Use rule reduction techniques such as address aggregation, or object grouping to reduce the number of rules to be added

Policy Difference Table:

Policy Diff Item	Source	Destination	Service	Cisco Rule Trails
161	10.0.0.0/8	192.168.9.0/24	tcp/5901	nat:nat/Default-Deny
181	172.17.0.0/16	192.168.9.0/24	tcp/5901	nat:nat/Default-Deny
181	172.16.0.0/16	192.168.9.0/24	tcp/5901	nat:nat/Default-Deny
199	192.168.3.0/24	192.168.9.0/24	tcp/5901	nat:nat/Default-Deny
199	192.168.4.0/24	192.168.9.0/24	tcp/5901	nat:nat/Default-Deny
199	192.168.2.0/24	192.168.9.0/24	tcp/5901	nat:nat/Default-Deny
199	192.168.5.0/24	192.168.9.0/24	tcp/5901	nat:nat/Default-Deny
238	10.0.0.0/8	192.168.1.0/24	tcp/5901	nat:nat/Default-Deny
239	172.17.0.0/16	192.168.1.0/24	tcp/5901	nat:nat/Default-Deny
240	192.168.4.0/24	192.168.1.0/24	tcp/5901	nat:nat/Default-Deny
240	192.168.2.0/24	192.168.1.0/24	tcp/5901	nat:nat/Default-Deny
240	192.168.5.0/24	192.168.1.0/24	tcp/5901	nat:nat/Default-Deny

Policy Diff Item	Source	Destination	Service	Cisco Rule Trails
240	192.168.3.0/24	192.168.1.0/24	tcp/5901	nat:nat/Default-Deny
275	192.168.5.0/24	192.168.50.3 to 192.168.50.255	tcp/5901	nat:nat/Default-Deny
275	192.168.4.0/24	192.168.50.3 to 192.168.50.255	tcp/5901	nat:nat/Default-Deny
275	192.168.5.0/24	192.168.50.0/31	tcp/5901	nat:nat/Default-Deny
275	192.168.4.0/24	192.168.50.0/31	tcp/5901	nat:nat/Default-Deny

Added policy caused by Checkpoint acl rule 28

Rule Index	Source	Destination	Service	VPN	Action	Comment
28	Migrated_inside_Interface	Any	udp-5901		accept	(Original ACE (line 85): access-list acl_inside permit udp any any eq 5901)

Cisco Overlap Rules:

Line No	Interface	Rule
	vpn4	high-to-low-default-allow
80	inside	access-list acl_inside permit udp host 192.168.5.251 any
82	inside	access-list acl_inside permit udp host 192.168.5.250 any
85	inside	access-list acl_inside permit udp any any eq 5901
91	inside	access-list acl_inside permit udp any any

Difference caused by:

NAT control in Cisco Device

Problem Source:

NAT control in Cisco devices limits access to packets which are associated with NAT rules. Thus, the source, destination addresses, or services of allowed packets are smaller than what is indicated by this Checkpoint rule.

Remedy based on allow policies:

The set of packets that are allowed in the Cisco device are shown in the Allow Policy Table. To use this table:

1. Replace this Checkpoint rule with allow rules for packets described in each row of the table.
2. Use rule reduction techniques such as address aggregation, or object grouping to reduce the number of rules to be added.

Allow Policy Table:

Service	Source	Destination
udp/5901	10.0.0.0/8	0.0.0.0 to 9.255.255.255 11.0.0.0 to 172.15.255.255

Service	Source	Destination
udp/5901	10.0.0.0/8	172.18.0.0 to 192.168.0.255 192.168.6.0 to 192.168.8.255 192.168.10.0 to 255.255.255.255
udp/5901	172.16.0.0/15	0.0.0.0 to 9.255.255.255 11.0.0.0 to 172.15.255.255 192.168.6.0 to 192.168.8.255 192.168.10.0 to 255.255.255.255
udp/5901	172.16.0.0/16	172.18.0.0 to 192.168.1.255
udp/5901	172.17.0.0/16	172.18.0.0 to 192.168.0.255
udp/5901	192.168.2.0 to 192.168.5.255	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
udp/5901	192.168.2.0/23	192.168.10.0 to 255.255.255.255
udp/5901	192.168.4.0/23	192.168.10.0 to 192.168.49.255 192.168.51.0 to 255.255.255.255

Remedy based on policy diff items:

The set of packets that are allowed by the Checkpoint device, but denied by the Cisco device, are shown in the Policy Difference Table. There may be multiple tables, each caused by a specific problem. The remedy is the following:

1. The Checkpoint rule should not be removed or altered.
2. Add rules above this Checkpoint rule to deny each packet described in the Policy Difference Table below.
3. Use rule reduction techniques such as address aggregation, or object grouping to reduce the number of rules to be added

Policy Difference Table:

Policy Diff Item	Source	Destination	Service	Cisco Rule Trails
166	10.0.0.0/8	192.168.9.0/24	udp/5901	nat:nat/Default-Deny
186	172.16.0.0/16	192.168.9.0/24	udp/5901	nat:nat/Default-Deny
186	172.17.0.0/16	192.168.9.0/24	udp/5901	nat:nat/Default-Deny
204	192.168.5.252/30	192.168.9.0/24	udp/5901	nat:nat/Default-Deny
204	192.168.4.0/24	192.168.9.0/24	udp/5901	nat:nat/Default-Deny
204	192.168.2.0/24	192.168.9.0/24	udp/5901	nat:nat/Default-Deny
204	192.168.5.0 to 192.168.5.249	192.168.9.0/24	udp/5901	nat:nat/Default-Deny
204	192.168.3.0/24	192.168.9.0/24	udp/5901	nat:nat/Default-Deny
253	10.0.0.0/8	192.168.1.0/24	udp/5901	nat:nat/Default-Deny
254	172.17.0.0/16	192.168.1.0/24	udp/5901	nat:nat/Default-Deny
255	192.168.3.0/24	192.168.1.0/24	udp/5901	nat:nat/Default-Deny
255	192.168.2.0/24	192.168.1.0/24	udp/5901	nat:nat/Default-Deny
255	192.168.4.0/24	192.168.1.0/24	udp/5901	nat:nat/Default-Deny
255	192.168.5.252/30	192.168.1.0/24	udp/5901	nat:nat/Default-Deny
255	192.168.5.0 to 192.168.5.249	192.168.1.0/24	udp/5901	nat:nat/Default-Deny

Policy Diff Item	Source	Destination	Service	Cisco Rule Trails
280	192.168.5.0 to 192.168.5.249	192.168.50.0/24	udp/5901	nat:nat/Default-Deny
280	192.168.5.252/30	192.168.50.0/24	udp/5901	nat:nat/Default-Deny
280	192.168.4.0/24	192.168.50.0/24	udp/5901	nat:nat/Default-Deny

Added policy caused by Checkpoint acl rule 29

Rule Index	Source	Destination	Service	VPN	Action	Comment
29	Migrated_inside_Interface	Any	cbt		accept	(Original ACE (line 86): access-list acl_inside permit tcp any any eq 7777)

Cisco Overlap Rules:

Line No	Interface	Rule
	vpn4	high-to-low-default-allow
86	inside	access-list acl_inside permit tcp any any eq 7777

Difference caused by:

NAT control in Cisco Device

Problem Source:

NAT control in Cisco devices limits access to packets which are associated with NAT rules. Thus, the source, destination addresses, or services of allowed packets are smaller than what is indicated by this Checkpoint rule.

Remedy based on allow policies:

The set of packets that are allowed in the Cisco device are shown in the Allow Policy Table. To use this table:

1. Replace this Checkpoint rule with allow rules for packets described in each row of the table.
2. Use rule reduction techniques such as address aggregation, or object grouping to reduce the number of rules to be added.

Allow Policy Table:

Service	Source	Destination
tcp/cbt	10.0.0.0/8	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 255.255.255.255
tcp/cbt	172.16.0.0/15	0.0.0.0 to 9.255.255.255 11.0.0.0 to 172.15.255.255 192.168.6.0 to 192.168.8.255 192.168.10.0 to 255.255.255.255
tcp/cbt	172.16.0.0/16	172.18.0.0 to 192.168.1.255

Service	Source	Destination
tcp/cbt	172.17.0.0/16	172.18.0.0 to 192.168.0.255
tcp/cbt	192.168.2.0 to 192.168.5.255	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
tcp/cbt	192.168.2.0/23	192.168.10.0 to 255.255.255.255
tcp/cbt	192.168.4.0/23	192.168.10.0 to 192.168.49.255 192.168.51.0 to 255.255.255.255

Remedy based on policy diff items:

The set of packets that are allowed by the Checkpoint device, but denied by the Cisco device, are shown in the Policy Difference Table. There may be multiple tables, each caused by a specific problem. The remedy is the following:

1. The Checkpoint rule should not be removed or altered.
2. Add rules above this Checkpoint rule to deny each packet described in the Policy Difference Table below.
3. Use rule reduction techniques such as address aggregation, or object grouping to reduce the number of rules to be added

Policy Difference Table:

Policy Diff Item	Source	Destination	Service	Cisco Rule Trails
163	10.0.0.0/8	192.168.9.0/24	tcp/cbt	nat:nat/Default-Deny
183	172.16.0.0/15	192.168.9.0/24	tcp/cbt	nat:nat/Default-Deny
201	192.168.2.0 to 192.168.5.255	192.168.9.0/24	tcp/cbt	nat:nat/Default-Deny
244	10.0.0.0/8	192.168.1.0/24	tcp/cbt	nat:nat/Default-Deny
245	172.17.0.0/16	192.168.1.0/24	tcp/cbt	nat:nat/Default-Deny
246	192.168.2.0 to 192.168.5.255	192.168.1.0/24	tcp/cbt	nat:nat/Default-Deny
277	192.168.4.0/23	192.168.50.0/24	tcp/cbt	nat:nat/Default-Deny

Added policy caused by Checkpoint acl rule 34

Rule Index	Source	Destination	Service	VPN	Action	Comment
34	Migrated_inside_Interface	Any	all_udp		accept	(Original ACE (line 91): access-list acl_inside permit udp any any)

Cisco Overlap Rules:

Line No	Interface	Rule
	vpn4	high-to-low-default-allow
106	testweb	access-list acl_testweb permit udp any any eq dnsix
108	testweb	access-list acl_testweb permit udp any any eq domain

Line No	Interface	Rule
67	inside	access-list acl_inside permit udp host 172.16.0.68 any eq domain
70	inside	access-list acl_inside permit udp host 172.16.0.68 any eq ntp
80	inside	access-list acl_inside permit udp host 192.168.5.251 any
82	inside	access-list acl_inside permit udp host 192.168.5.250 any
85	inside	access-list acl_inside permit udp any any eq 5901
87	inside	access-list acl_inside permit udp any host 172.16.0.4 eq ntp
91	inside	access-list acl_inside permit udp any any

Difference caused by:

NAT control in Cisco Device

Problem Source:

NAT control in Cisco devices limits access to packets which are associated with NAT rules. Thus, the source, destination addresses, or services of allowed packets are smaller than what is indicated by this Checkpoint rule.

Remedy based on allow policies:

The set of packets that are allowed in the Cisco device are shown in the Allow Policy Table. To use this table:

1. Replace this Checkpoint rule with allow rules for packets described in each row of the table.
2. Use rule reduction techniques such as address aggregation, or object grouping to reduce the number of rules to be added.

Allow Policy Table:

Service	Source	Destination
udp/any	10.0.0.0/8	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 255.255.255.255
udp/any	172.16.0.0/15	0.0.0.0 to 9.255.255.255 11.0.0.0 to 172.15.255.255 192.168.6.0 to 192.168.8.255 192.168.10.0 to 255.255.255.255
udp/any	172.16.0.0/16	172.18.0.0 to 192.168.1.255
udp/any	172.17.0.0/16	172.18.0.0 to 192.168.0.255
udp/any	192.168.2.0 to 192.168.5.255	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
udp/any	192.168.2.0/23	192.168.10.0 to 255.255.255.255
udp/any	192.168.4.0/23	192.168.10.0 to 192.168.49.255 192.168.51.0 to 255.255.255.255
udp/rsh	172.16.0.1	172.16.0.200
udp/snmp	172.16.0.61	172.16.0.1
udp/snmptrap	172.16.0.1	172.16.0.61

Remedy based on policy diff items:

The set of packets that are allowed by the Checkpoint device, but denied by the Cisco device, are shown in the Policy Difference Table. There may be multiple tables, each caused by a specific problem. The remedy is the following:

1. The Checkpoint rule should not be removed or altered.
2. Add rules above this Checkpoint rule to deny each packet described in the Policy Difference Table below.
3. Use rule reduction techniques such as address aggregation, or object grouping to reduce the number of rules to be added

Policy Difference Table:

Policy Diff Item	Source	Destination	Service	Cisco Rule Trails
166	10.0.0.0/8	192.168.9.0/24	udp/5902-65535	nat:nat/Default-Deny
166	10.0.0.0/8	192.168.9.0/24	udp/1-5900	nat:nat/Default-Deny
186	172.16.0.68	192.168.9.0/24	udp/54-122	nat:nat/Default-Deny
186	172.16.0.0/16	192.168.9.0/24	udp/5902-65535	nat:nat/Default-Deny
186	172.17.0.0/16	192.168.9.0/24	udp/5902-65535	nat:nat/Default-Deny
186	172.17.0.0/16	192.168.9.0/24	udp/1-5900	nat:nat/Default-Deny
186	172.16.0.69 to 172.16.255.255	192.168.9.0/24	udp/1-5900	nat:nat/Default-Deny
186	172.16.0.68	192.168.9.0/24	udp/1-52	nat:nat/Default-Deny
186	172.16.0.0 to 172.16.0.67	192.168.9.0/24	udp/1-5900	nat:nat/Default-Deny
186	172.16.0.68	192.168.9.0/24	udp/124-5900	nat:nat/Default-Deny
204	192.168.2.0/24	192.168.9.0/24	udp/1-5900	nat:nat/Default-Deny
204	192.168.4.0/24	192.168.9.0/24	udp/5902-65535	nat:nat/Default-Deny
204	192.168.5.0 to 192.168.5.249	192.168.9.0/24	udp/1-5900	nat:nat/Default-Deny
204	192.168.4.0/24	192.168.9.0/24	udp/1-5900	nat:nat/Default-Deny
204	192.168.5.252/30	192.168.9.0/24	udp/5902-65535	nat:nat/Default-Deny
204	192.168.3.0/24	192.168.9.0/24	udp/1-5900	nat:nat/Default-Deny
204	192.168.5.252/30	192.168.9.0/24	udp/1-5900	nat:nat/Default-Deny
204	192.168.3.0/24	192.168.9.0/24	udp/5902-65535	nat:nat/Default-Deny
204	192.168.2.0/24	192.168.9.0/24	udp/5902-65535	nat:nat/Default-Deny
204	192.168.5.0 to 192.168.5.249	192.168.9.0/24	udp/5902-65535	nat:nat/Default-Deny
253	10.0.0.0/8	192.168.1.0/24	udp/1-5900	nat:nat/Default-Deny
253	10.0.0.0/8	192.168.1.0/24	udp/5902-65535	nat:nat/Default-Deny
254	172.17.0.0/16	192.168.1.0/24	udp/5902-65535	nat:nat/Default-Deny
254	172.17.0.0/16	192.168.1.0/24	udp/1-5900	nat:nat/Default-Deny
255	192.168.5.0 to 192.168.5.249	192.168.1.0/24	udp/5902-65535	nat:nat/Default-Deny
255	192.168.4.0/24	192.168.1.0/24	udp/5902-65535	nat:nat/Default-Deny
255	192.168.3.0/24	192.168.1.0/24	udp/5902-65535	nat:nat/Default-Deny
255	192.168.4.0/24	192.168.1.0/24	udp/1-5900	nat:nat/Default-Deny
255	192.168.5.0 to 192.168.5.249	192.168.1.0/24	udp/1-5900	nat:nat/Default-Deny
255	192.168.2.0/24	192.168.1.0/24	udp/5902-65535	nat:nat/Default-Deny
255	192.168.5.252/30	192.168.1.0/24	udp/5902-65535	nat:nat/Default-Deny

Policy Diff Item	Source	Destination	Service	Cisco Rule Trails
255	192.168.2.0/24	192.168.1.0/24	udp/1-5900	nat:nat/Default-Deny
255	192.168.3.0/24	192.168.1.0/24	udp/1-5900	nat:nat/Default-Deny
255	192.168.5.252/30	192.168.1.0/24	udp/1-5900	nat:nat/Default-Deny
280	192.168.5.0 to 192.168.5.249	192.168.50.0/24	udp/5902-65535	nat:nat/Default-Deny
280	192.168.5.252/30	192.168.50.0/24	udp/1-5900	nat:nat/Default-Deny
280	192.168.4.0/24	192.168.50.0/24	udp/5902-65535	nat:nat/Default-Deny
280	192.168.4.0/24	192.168.50.0/24	udp/1-5900	nat:nat/Default-Deny
280	192.168.5.252/30	192.168.50.0/24	udp/5902-65535	nat:nat/Default-Deny
280	192.168.5.0 to 192.168.5.249	192.168.50.0/24	udp/1-5900	nat:nat/Default-Deny

Deleted policy caused by Checkpoint acl rule 35

Rule Index	Source	Destination	Service	VPN	Action	Comment
35	Migrated_inside_Interface	Any	Any		drop	Auto-generated implied any any drop rule at end of ACL

Cisco Overlap Rules:

Line No	Interface	Rule
	any	implied-icmp-deny
61	inside	access-list acl_inside deny tcp host 172.16.0.24 any eq ftp
62	inside	access-list acl_inside deny tcp host 172.16.0.24 any eq ssh
76	inside	access-list acl_inside deny tcp host 172.16.0.19 any eq ftp
77	inside	access-list acl_inside deny tcp host 172.16.0.19 any eq ssh
89	inside	access-list acl_inside deny tcp host 172.16.0.15 any eq ftp
90	inside	access-list acl_inside deny tcp host 172.16.0.15 any eq ssh

Difference caused by:

ACL rules with deny action and "any" only in destination

Problem Source:

There might be two reasons for this case, which are easily identifiable from the Cisco acl match/overlap rule table above:

1. Improper translation

There is no matching rule, but there are overlap rules: source or service field may be an incorrect translation. If policy difference-based remedy proposed below results in a large number of added rules, an alternative remedy is to correct the incorrectly translated field, if that can be identified. You might have to run this report again to ensure that the fix is complete.

2. Zone spanning

Here is an exact match with a Cisco rule, yet the Cisco rule may have its source include networks that are not reachable from the corresponding interface. They are harmless in the Cisco context but can cause additional allow or deny policies in Checkpoint.

Remedy:

Identify the source addresses that are specified in this Checkpoint rule and that are part of the reachable networks in the reachability table. Replace the source address in this Checkpoint rule with only those source addresses.

Refer to [Cisco Reachability Table](#)

Remedy based on policy diff items:

The set of packets that are denied by the Checkpoint device, but allowed by the Cisco device, are shown in the Policy Difference Table. There may be multiple tables, each caused by a specific problem. The remedy is the following:

1. The Checkpoint rule should not be removed or altered.
2. Add rules above this Checkpoint rule to allow packets described in each row of the Policy Difference Table below.
3. Use rule reduction techniques such as address aggregation, or object grouping to reduce the number of rules to be added

Policy Difference Table:

Policy Diff Item	Source	Destination	Service	Cisco Rule Trails
256	172.16.0.0/16	192.168.1.0/24	icmp	acl:78
261	172.16.0.0/16	192.168.1.0/24	tcp/h323	acl:79
281	10.0.0.0/8	192.168.50.0/24	icmp	acl:78
286	172.16.0.0/15	192.168.50.0/24	icmp	acl:78
291	192.168.2.0/23	192.168.50.0/24	icmp	acl:78
296	10.0.0.0/8	192.168.50.0/24	tcp/h323	acl:79
297	172.16.0.0/15	192.168.50.0/24	tcp/h323	acl:79
298	192.168.2.0/23	192.168.50.0/24	tcp/h323	acl:79
317	10.0.0.0/8	0.0.0.0 to 9.255.255.255	icmp	acl:78
322	10.0.0.0/8	11.0.0.0 to 172.15.255.255	icmp	acl:78
327	10.0.0.0/8	172.18.0.0 to 192.168.0.255	icmp	acl:78
332	10.0.0.0/8	192.168.6.0 to 192.168.8.255	icmp	acl:78
337	10.0.0.0/8	192.168.10.0 to 192.168.49.255	icmp	acl:78
342	10.0.0.0/8	192.168.51.0 to 255.255.255.255	icmp	acl:78
347	172.16.0.0/15	0.0.0.0 to 9.255.255.255	icmp	acl:78
352	172.16.0.0/15	11.0.0.0 to 172.15.255.255	icmp	acl:78
357	172.16.0.0/15	172.18.0.0 to 192.168.0.255	icmp	acl:78
362	172.16.0.0/15	192.168.6.0 to 192.168.8.255	icmp	acl:78
367	172.16.0.0/15	192.168.10.0 to 192.168.49.255	icmp	acl:78
372	172.16.0.0/15	192.168.51.0 to 255.255.255.255	icmp	acl:78
377	192.168.2.0 to 192.168.5.255	0.0.0.0 to 9.255.255.255	icmp	acl:78
382	192.168.2.0 to 192.168.5.255	11.0.0.0 to 172.15.255.255	icmp	acl:78

Policy Diff Item	Source	Destination	Service	Cisco Rule Trails
387	192.168.2.0 to 192.168.5.255	172.18.0.0 to 192.168.0.255	icmp	acl:78
392	192.168.2.0 to 192.168.5.255	192.168.6.0 to 192.168.8.255	icmp	acl:78
397	192.168.2.0 to 192.168.5.255	192.168.10.0 to 192.168.49.255	icmp	acl:78
402	192.168.2.0 to 192.168.5.255	192.168.51.0 to 255.255.255.255	icmp	acl:78
407	10.0.0.0/8	0.0.0.0 to 9.255.255.255	tcp/h323	acl:79
408	10.0.0.0/8	11.0.0.0 to 172.15.255.255	tcp/h323	acl:79
409	10.0.0.0/8	172.18.0.0 to 192.168.0.255	tcp/h323	acl:79
410	10.0.0.0/8	192.168.6.0 to 192.168.8.255	tcp/h323	acl:79
411	10.0.0.0/8	192.168.10.0 to 192.168.49.255	tcp/h323	acl:79
412	10.0.0.0/8	192.168.51.0 to 255.255.255.255	tcp/h323	acl:79
413	172.16.0.0/15	0.0.0.0 to 9.255.255.255	tcp/h323	acl:79
414	172.16.0.0/15	11.0.0.0 to 172.15.255.255	tcp/h323	acl:79
415	172.16.0.0/15	172.18.0.0 to 192.168.0.255	tcp/h323	acl:79
416	172.16.0.0/15	192.168.6.0 to 192.168.8.255	tcp/h323	acl:79
417	172.16.0.0/15	192.168.10.0 to 192.168.49.255	tcp/h323	acl:79
418	172.16.0.0/15	192.168.51.0 to 255.255.255.255	tcp/h323	acl:79
419	192.168.2.0 to 192.168.5.255	0.0.0.0 to 9.255.255.255	tcp/h323	acl:79
420	192.168.2.0 to 192.168.5.255	11.0.0.0 to 172.15.255.255	tcp/h323	acl:79
421	192.168.2.0 to 192.168.5.255	172.18.0.0 to 192.168.0.255	tcp/h323	acl:79
422	192.168.2.0 to 192.168.5.255	192.168.6.0 to 192.168.8.255	tcp/h323	acl:79
423	192.168.2.0 to 192.168.5.255	192.168.10.0 to 192.168.49.255	tcp/h323	acl:79
424	192.168.2.0 to 192.168.5.255	192.168.51.0 to 255.255.255.255	tcp/h323	acl:79

Added policy caused by Checkpoint acl rule 37

Rule Index	Source	Destination	Service	VPN	Action	Comment
37	Migrated_sjpix_vpn4_Interface	mail1_reachable_nets	Any		accept	Auto-generated implied ACL for high security interface (vpn4: security level 80) to low security interface (mail1: security level 50) traffic

Cisco Overlap Rules:

Line No	Interface	Rule
	vpn4	high-to-low-default-allow
102	testweb	access-list acl_testweb permit tcp any any eq www
103	testweb	access-list acl_testweb permit tcp any any eq https
104	testweb	access-list acl_testweb permit tcp any any eq ssh
105	testweb	access-list acl_testweb permit tcp any any eq smtp
106	testweb	access-list acl_testweb permit udp any any eq dnsix
107	testweb	access-list acl_testweb permit icmp any any
108	testweb	access-list acl_testweb permit udp any any eq domain
109	proxymail	access-list acl_proxymail permit tcp any any eq www
110	proxymail	access-list acl_proxymail permit tcp any any eq https
111	proxymail	access-list acl_proxymail permit icmp any any
53	mail1	access-list acl_mail1 permit tcp any host 192.168.1.4 eq smtp
56	mail1	access-list acl_mail1 permit tcp any any eq www
57	mail1	access-list acl_mail1 permit tcp any any eq https
58	inside	access-list acl_inside permit tcp any any eq www
59	inside	access-list acl_inside permit tcp any any eq https
60	inside	access-list acl_inside permit tcp any any eq 5405
63	inside	access-list acl_inside permit tcp any any eq ftp
64	inside	access-list acl_inside permit tcp any any eq ssh
65	inside	access-list acl_inside permit tcp any any eq 81
66	inside	access-list acl_inside permit tcp any any eq telnet
68	inside	access-list acl_inside permit tcp any any eq 9895
69	inside	access-list acl_inside permit tcp any any eq nntp
73	inside	access-list acl_inside permit tcp any any eq 7618
74	inside	access-list acl_inside permit tcp any any eq 8080
78	inside	access-list acl_inside permit icmp any any
79	inside	access-list acl_inside permit tcp any any eq h323
81	inside	access-list acl_inside permit tcp any any eq 5900
84	inside	access-list acl_inside permit tcp any any eq 5901
85	inside	access-list acl_inside permit udp any any eq 5901

Line No	Interface	Rule
86	inside	access-list acl_inside permit tcp any any eq 7777
91	inside	access-list acl_inside permit udp any any

Difference caused by:

ACL Allow rules with specific source and destination address

Problem Source:

There might be three reasons for this case, that are easily identifiable from the Cisco acl rule table above:

- 1) Improper source or destination translation
 There is no matching rule, but there are overlap rules: source or destination field may be an incorrect translation. If both remedies proposed below result in a large number of added rules, an alternative remedy is to correct the incorrectly translated field, if that can be identified. You might have to run this report again to ensure that the fix is complete.
- 2) Zone spanning
 Here is an exact match with a Cisco rule, yet the Cisco rule may have its source include networks that are not reachable from the corresponding interface. They are harmless in the Cisco context but can cause additional allow policies in Checkpoint.
- 3) Irrelevant rules
 There are no matching/overlap Cisco rules; the Checkpoint rule may be added arbitrarily or may be an incorrect translation.

Remedy:

- 1) Improper source or destination translation
 - a. Using Cisco overlap rules to identify improperly translated field(s), correct those field as appropriate.
- 2) Zone spanning
 - a. Use the interfaces shown in the Cisco matching/overlap rule table above, to locate them in the Interface column of the Cisco Reachability table at the end of this report, and read the source addresses in the "Reachable Networks" column of that table corresponding to the interfaces that were located. Replace the source address in this Checkpoint rule with only those source addresses.
- 3) Irrelevant rules
 There are no matching or overlap Cisco rules - remove this Checkpoint rule.

Remedy based on policy diff items:

The set of packets that are allowed by the Checkpoint device, but denied by the Cisco device, are shown in the Policy Difference Table. There may be multiple tables, each caused by a specific problem. The remedy is the following:

- 1. The Checkpoint rule should not be removed or altered.
- 2. Add rules above this Checkpoint rule to deny each packet described in the Policy Difference Table below.
- 3. Use rule reduction techniques such as address aggregation, or object grouping to reduce the number of rules to be added

Policy Difference Table:

Policy Diff Item	Source	Destination	Service	Cisco Rule Trails
580	127.0.0.1	192.168.1.0/24	any	acl:access-list-acl_outside- implied-deny

Added policy caused by Checkpoint acl rule 38

Rule Index	Source	Destination	Service	VPN	Action	Comment
38	Migrated_sjpix_vpn4_Interface	testweb_reachable_nets	Any		accept	Auto-generated implied ACL for high security interface (vpn4: security level 80) to low security interface (testweb: security level 10) traffic

Cisco Overlap Rules:

Line No	Interface	Rule
	vpn4	high-to-low-default-allow
102	testweb	access-list acl_testweb permit tcp any any eq www
103	testweb	access-list acl_testweb permit tcp any any eq https
104	testweb	access-list acl_testweb permit tcp any any eq ssh
105	testweb	access-list acl_testweb permit tcp any any eq smtp
106	testweb	access-list acl_testweb permit udp any any eq dnsix
107	testweb	access-list acl_testweb permit icmp any any
108	testweb	access-list acl_testweb permit udp any any eq domain
109	proxymail	access-list acl_proxymail permit tcp any any eq www
110	proxymail	access-list acl_proxymail permit tcp any any eq https
111	proxymail	access-list acl_proxymail permit icmp any any
56	mail1	access-list acl_mail1 permit tcp any any eq www
57	mail1	access-list acl_mail1 permit tcp any any eq https
58	inside	access-list acl_inside permit tcp any any eq www
59	inside	access-list acl_inside permit tcp any any eq https
60	inside	access-list acl_inside permit tcp any any eq 5405
63	inside	access-list acl_inside permit tcp any any eq ftp
64	inside	access-list acl_inside permit tcp any any eq ssh
65	inside	access-list acl_inside permit tcp any any eq 81
66	inside	access-list acl_inside permit tcp any any eq telnet
68	inside	access-list acl_inside permit tcp any any eq 9895
69	inside	access-list acl_inside permit tcp any any eq nntp
73	inside	access-list acl_inside permit tcp any any eq 7618
74	inside	access-list acl_inside permit tcp any any eq 8080
78	inside	access-list acl_inside permit icmp any any
79	inside	access-list acl_inside permit tcp any any eq h323
81	inside	access-list acl_inside permit tcp any any eq 5900

Line No	Interface	Rule
83	inside	access-list acl_inside permit tcp any host 192.168.50.2 eq 5901
84	inside	access-list acl_inside permit tcp any any eq 5901
85	inside	access-list acl_inside permit udp any any eq 5901
86	inside	access-list acl_inside permit tcp any any eq 7777
91	inside	access-list acl_inside permit udp any any

Difference caused by:

ACL Allow rules with specific source and destination address

Problem Source:

There might be three reasons for this case, that are easily identifiable from the Cisco acl rule table above:

- 1) Improper source or destination translation
There is no matching rule, but there are overlap rules: source or destination field may be an incorrect translation. If both remedies proposed below result in a large number of added rules, an alternative remedy is to correct the incorrectly translated field, if that can be identified. You might have to run this report again to ensure that the fix is complete.
- 2) Zone spanning
Here is an exact match with a Cisco rule, yet the Cisco rule may have its source include networks that are not reachable from the corresponding interface. They are harmless in the Cisco context but can cause additional allow policies in Checkpoint.
- 3) Irrelevant rules
There are no matching/overlap Cisco rules; the Checkpoint rule may be added arbitrarily or may be an incorrect translation.

Remedy:

- 1) Improper source or destination translation
 - a. Using Cisco overlap rules to identify improperly translated field(s), correct those field as appropriate.
- 2) Zone spanning
 - a. Use the interfaces shown in the Cisco matching/overlap rule table above, to locate them in the Interface column of the Cisco Reachability table at the end of this report, and read the source addresses in the "Reachable Networks" column of that table corresponding to the interfaces that were located. Replace the source address in this Checkpoint rule with only those source addresses.
- 3) Irrelevant rules
There are no matching or overlap Cisco rules - remove this Checkpoint rule.

Remedy based on policy diff items:

The set of packets that are allowed by the Checkpoint device, but denied by the Cisco device, are shown in the Policy Difference Table. There may be multiple tables, each caused by a specific problem. The remedy is the following:

1. The Checkpoint rule should not be removed or altered.
2. Add rules above this Checkpoint rule to deny each packet described in the Policy Difference Table below.
3. Use rule reduction techniques such as address aggregation, or object grouping to reduce the number of rules to be added

Policy Difference Table:

Policy Diff Item	Source	Destination	Service	Cisco Rule Trails
588	127.0.0.1	192.168.50.0/24	any	acl:access-list-acl_outside- implied-deny

Added policy caused by Checkpoint acl rule 39

Rule Index	Source	Destination	Service	VPN	Action	Comment
39	Migrated_sjpix_vpn4_Interface	proxymail_reachable_nets	Any		accept	Auto-generated implied ACL for high security interface (vpn4: security level 80) to low security interface (proxymail: security level 20) traffic

Cisco Overlap Rules:

Line No	Interface	Rule
	vpn4	high-to-low-default-allow
102	testweb	access-list acl_testweb permit tcp any any eq www
103	testweb	access-list acl_testweb permit tcp any any eq https
104	testweb	access-list acl_testweb permit tcp any any eq ssh
105	testweb	access-list acl_testweb permit tcp any any eq smtp
106	testweb	access-list acl_testweb permit udp any any eq dnsix
107	testweb	access-list acl_testweb permit icmp any any
108	testweb	access-list acl_testweb permit udp any any eq domain
109	proxymail	access-list acl_proxymail permit tcp any any eq www
110	proxymail	access-list acl_proxymail permit tcp any any eq https
111	proxymail	access-list acl_proxymail permit icmp any any
56	mail1	access-list acl_mail1 permit tcp any any eq www
57	mail1	access-list acl_mail1 permit tcp any any eq https
58	inside	access-list acl_inside permit tcp any any eq www
59	inside	access-list acl_inside permit tcp any any eq https
60	inside	access-list acl_inside permit tcp any any eq 5405
63	inside	access-list acl_inside permit tcp any any eq ftp
64	inside	access-list acl_inside permit tcp any any eq ssh
65	inside	access-list acl_inside permit tcp any any eq 81
66	inside	access-list acl_inside permit tcp any any eq telnet
68	inside	access-list acl_inside permit tcp any any eq 9895
69	inside	access-list acl_inside permit tcp any any eq nntp

Line No	Interface	Rule
73	inside	access-list acl_inside permit tcp any any eq 7618
74	inside	access-list acl_inside permit tcp any any eq 8080
78	inside	access-list acl_inside permit icmp any any
79	inside	access-list acl_inside permit tcp any any eq h323
81	inside	access-list acl_inside permit tcp any any eq 5900
84	inside	access-list acl_inside permit tcp any any eq 5901
85	inside	access-list acl_inside permit udp any any eq 5901
86	inside	access-list acl_inside permit tcp any any eq 7777
91	inside	access-list acl_inside permit udp any any

Difference caused by:

ACL Allow rules with specific source and destination address

Problem Source:

There might be three reasons for this case, that are easily identifiable from the Cisco acl rule table above:

- 1) Improper source or destination translation
There is no matching rule, but there are overlap rules: source or destination field may be an incorrect translation. If both remedies proposed below result in a large number of added rules, an alternative remedy is to correct the incorrectly translated field, if that can be identified. You might have to run this report again to ensure that the fix is complete.
- 2) Zone spanning
Here is an exact match with a Cisco rule, yet the Cisco rule may have its source include networks that are not reachable from the corresponding interface. They are harmless in the Cisco context but can cause additional allow policies in Checkpoint.
- 3) Irrelevant rules
There are no matching/overlap Cisco rules; the Checkpoint rule may be added arbitrarily or may be an incorrect translation.

Remedy:

- 1) Improper source or destination translation
 - a. Using Cisco overlap rules to identify improperly translated field(s), correct those field as appropriate.
- 2) Zone spanning
 - a. Use the interfaces shown in the Cisco matching/overlap rule table above, to locate them in the Interface column of the Cisco Reachability table at the end of this report, and read the source addresses in the "Reachable Networks" column of that table corresponding to the interfaces that were located. Replace the source address in this Checkpoint rule with only those source addresses.
- 3) Irrelevant rules
There are no matching or overlap Cisco rules - remove this Checkpoint rule.

Remedy based on policy diff items:

The set of packets that are allowed by the Checkpoint device, but denied by the Cisco device, are shown in the Policy Difference Table. There may be multiple tables, each caused by a specific problem. The remedy is the following:

1. The Checkpoint rule should not be removed or altered.
2. Add rules above this Checkpoint rule to deny each packet described in the Policy Difference Table below.
3. Use rule reduction techniques such as address aggregation, or object grouping to reduce the number of rules to be added

Policy Difference Table:

Policy Diff Item	Source	Destination	Service	Cisco Rule Trails
538	127.0.0.1	192.168.9.0/24	any	acl:access-list-acl_outside- implied-deny

Added policy caused by Checkpoint acl rule 41

Rule Index	Source	Destination	Service	VPN	Action	Comment
41	Host_192.168.1.2	Any	smtp		accept	(Original ACE (line 54): access-list acl_mail1 permit tcp host 192.168.1.2 any eq smtp)

Cisco Matching Rules:

Line No	Interface	Rule
54	mail1	access-list acl_mail1 permit tcp host 192.168.1.2 any eq smtp

Difference caused by:

NAT control in Cisco Device

Problem Source:

NAT control in Cisco devices limits access to packets which are associated with NAT rules. Thus, the source, destination addresses, or services of allowed packets are smaller than what is indicated by this Checkpoint rule.

Remedy based on allow policies:

The set of packets that are allowed in the Cisco device are shown in the Allow Policy Table. To use this table:

1. Replace this Checkpoint rule with allow rules for packets described in each row of the table.
2. Use rule reduction techniques such as address aggregation, or object grouping to reduce the number of rules to be added.

Allow Policy Table:

Service	Source	Destination
tcp/smtp	192.168.1.2	0.0.0.0 to 9.255.255.255 11.0.0.0 to 172.15.255.255 172.18.0.0 to 192.168.0.255 192.168.1.4 192.168.6.0 to 192.168.8.255 192.168.10.0 to 255.255.255.255

Remedy based on policy diff items:

The set of packets that are allowed by the Checkpoint device, but denied by the Cisco device, are shown in the Policy Difference Table. There may be multiple tables, each caused by a specific problem. The remedy is the following:

1. The Checkpoint rule should not be removed or altered.
2. Add rules above this Checkpoint rule to deny each packet described in the Policy Difference Table below.
3. Use rule reduction techniques such as address aggregation, or object grouping to reduce the number of rules to be added

Policy Difference Table:

Policy Diff Item	Source	Destination	Service	Cisco Rule Trails
425	192.168.1.2	192.168.9.0/24	tcp/smtp	nat:nat/Default-Deny
429	192.168.1.2	10.0.0.0/8	tcp/smtp	nat:nat/Default-Deny
430	192.168.1.2	172.16.0.0/15	tcp/smtp	nat:nat/Default-Deny
431	192.168.1.2	192.168.2.0 to 192.168.5.255	tcp/smtp	nat:nat/Default-Deny

Added policy caused by Checkpoint acl rule 42

Rule Index	Source	Destination	Service	VPN	Action	Comment
42	Host_192.168.1.2	Any	domain-udp		accept	(Original ACE (line 55): access-list acl_mail1 permit udp host 192.168.1.2 any eq domain)

Cisco Matching Rules:

Line No	Interface	Rule
55	mail1	access-list acl_mail1 permit udp host 192.168.1.2 any eq domain

Difference caused by:

NAT control in Cisco Device

Problem Source:

NAT control in Cisco devices limits access to packets which are associated with NAT rules. Thus, the source, destination addresses, or services of allowed packets are smaller than what is indicated by this Checkpoint rule.

Remedy based on allow policies:

The set of packets that are allowed in the Cisco device are shown in the Allow Policy Table. To use this table:

1. Replace this Checkpoint rule with allow rules for packets described in each row of the table.
2. Use rule reduction techniques such as address aggregation, or object grouping to reduce the number of rules to be added.

Allow Policy Table:

Service	Source	Destination
udp/domain	192.168.1.2	0.0.0.0 to 9.255.255.255 11.0.0.0 to 172.15.255.255 172.18.0.0 to 192.168.0.255 192.168.1.4 192.168.6.0 to 192.168.8.255 192.168.10.0 to 255.255.255.255

Remedy based on policy diff items:

The set of packets that are allowed by the Checkpoint device, but denied by the Cisco device, are shown in the Policy Difference Table. There may be multiple tables, each caused by a specific problem. The remedy is the following:

1. The Checkpoint rule should not be removed or altered.
2. Add rules above this Checkpoint rule to deny each packet described in the Policy Difference Table below.
3. Use rule reduction techniques such as address aggregation, or object grouping to reduce the number of rules to be added

Policy Difference Table:

Policy Diff Item	Source	Destination	Service	Cisco Rule Trails
426	192.168.1.2	192.168.9.0/24	udp/domain	nat:nat/Default-Deny
438	192.168.1.2	10.0.0.0/8	udp/domain	nat:nat/Default-Deny
439	192.168.1.2	172.16.0.0/15	udp/domain	nat:nat/Default-Deny
440	192.168.1.2	192.168.2.0 to 192.168.5.255	udp/domain	nat:nat/Default-Deny

Added policy caused by Checkpoint acl rule 43

Rule Index	Source	Destination	Service	VPN	Action	Comment
43	mail1_reachable_nets	Any	http		accept	(Original ACE (line 56): access-list acl_mail1 permit tcp any any eq www)

Cisco Overlap Rules:

Line No	Interface	Rule
	vpn4	high-to-low-default-allow
102	testweb	access-list acl_testweb permit tcp any any eq www
109	proxymail	access-list acl_proxymail permit tcp any any eq www
35	outside	access-list acl_outside permit tcp any host 62.59.14.161 eq www
40	outside	access-list acl_outside permit tcp any host 62.59.14.170 eq www
41	outside	access-list acl_outside permit tcp any host 62.59.14.171 eq www

Line No	Interface	Rule
52	outside	access-list acl_outside permit tcp any host 62.59.14.169 eq www
56	mail1	access-list acl_mail1 permit tcp any any eq www
58	inside	access-list acl_inside permit tcp any any eq www

Difference caused by:

NAT control in Cisco Device

Problem Source:

NAT control in Cisco devices limits access to packets which are associated with NAT rules. Thus, the source, destination addresses, or services of allowed packets are smaller than what is indicated by this Checkpoint rule.

Remedy based on allow policies:

The set of packets that are allowed in the Cisco device are shown in the Allow Policy Table. To use this table:

1. Replace this Checkpoint rule with allow rules for packets described in each row of the table.
2. Use rule reduction techniques such as address aggregation, or object grouping to reduce the number of rules to be added.

Allow Policy Table:

Service	Source	Destination
tcp/http	192.168.1.0/24	0.0.0.0 to 9.255.255.255 11.0.0.0 to 172.15.255.255 172.18.0.0 to 192.168.0.255 192.168.1.4 192.168.6.0 to 192.168.8.255 192.168.10.0 to 255.255.255.255

Remedy based on policy diff items:

The set of packets that are allowed by the Checkpoint device, but denied by the Cisco device, are shown in the Policy Difference Table. There may be multiple tables, each caused by a specific problem. The remedy is the following:

1. The Checkpoint rule should not be removed or altered.
2. Add rules above this Checkpoint rule to deny each packet described in the Policy Difference Table below.
3. Use rule reduction techniques such as address aggregation, or object grouping to reduce the number of rules to be added

Policy Difference Table:

Policy Diff Item	Source	Destination	Service	Cisco Rule Trails
427	192.168.1.0/24	192.168.9.0/24	tcp/http	nat:nat/Default-Deny
432	192.168.1.0/24	10.0.0.0/8	tcp/http	nat:nat/Default-Deny
433	192.168.1.0/24	172.16.0.0/15	tcp/http	nat:nat/Default-Deny
434	192.168.1.0/24	192.168.2.0 to 192.168.5.255	tcp/http	nat:nat/Default-Deny

Added policy caused by Checkpoint acl rule 44

Rule Index	Source	Destination	Service	VPN	Action	Comment
44	mail1_reachable_networks	Any	https		accept	(Original ACE (line 57): access-list acl_mail1 permit tcp any any eq https)

Cisco Overlap Rules:

Line No	Interface	Rule
	vpn4	high-to-low-default-allow
103	testweb	access-list acl_testweb permit tcp any any eq https
110	proxymail	access-list acl_proxymail permit tcp any any eq https
36	outside	access-list acl_outside permit tcp any host 62.59.14.161 eq https
42	outside	access-list acl_outside permit tcp any host 62.59.14.171 eq https
51	outside	access-list acl_outside permit tcp any host 62.59.14.169 eq https
57	mail1	access-list acl_mail1 permit tcp any any eq https
59	inside	access-list acl_inside permit tcp any any eq https

Difference caused by:

NAT control in Cisco Device

Problem Source:

NAT control in Cisco devices limits access to packets which are associated with NAT rules. Thus, the source, destination addresses, or services of allowed packets are smaller than what is indicated by this Checkpoint rule.

Remedy based on allow policies:

The set of packets that are allowed in the Cisco device are shown in the Allow Policy Table. To use this table:

1. Replace this Checkpoint rule with allow rules for packets described in each row of the table.
2. Use rule reduction techniques such as address aggregation, or object grouping to reduce the number of rules to be added.

Allow Policy Table:

Service	Source	Destination
tcp/https	192.168.1.0/24	0.0.0.0 to 9.255.255.255 11.0.0.0 to 172.15.255.255 172.18.0.0 to 192.168.0.255 192.168.1.4 192.168.6.0 to 192.168.8.255 192.168.10.0 to 255.255.255.255

Remedy based on policy diff items:

The set of packets that are allowed by the Checkpoint device, but denied by the Cisco device, are shown in the Policy Difference Table. There may be multiple tables, each caused by a specific problem. The remedy is the following:

1. The Checkpoint rule should not be removed or altered.
2. Add rules above this Checkpoint rule to deny each packet described in the Policy Difference Table below.
3. Use rule reduction techniques such as address aggregation, or object grouping to reduce the number of rules to be added

Policy Difference Table:

Policy Diff Item	Source	Destination	Service	Cisco Rule Trails
428	192.168.1.0/24	192.168.9.0/24	tcp/https	nat:nat/Default-Deny
435	192.168.1.0/24	10.0.0.0/8	tcp/https	nat:nat/Default-Deny
436	192.168.1.0/24	172.16.0.0/15	tcp/https	nat:nat/Default-Deny
437	192.168.1.0/24	192.168.2.0 to 192.168.5.255	tcp/https	nat:nat/Default-Deny

Added policy caused by Checkpoint acl rule 46

Rule Index	Source	Destination	Service	VPN	Action	Comment
46	proxymail_reachable_nets	Any	http		accept	(Original ACE (line 109): access-list acl_proxymail permit tcp any any eq www)

Cisco Overlap Rules:

Line No	Interface	Rule
	vpn4	high-to-low-default-allow
102	testweb	access-list acl_testweb permit tcp any any eq www
109	proxymail	access-list acl_proxymail permit tcp any any eq www
35	outside	access-list acl_outside permit tcp any host 62.59.14.161 eq www
40	outside	access-list acl_outside permit tcp any host 62.59.14.170 eq www
41	outside	access-list acl_outside permit tcp any host 62.59.14.171 eq www
52	outside	access-list acl_outside permit tcp any host 62.59.14.169 eq www
56	mail1	access-list acl_mail1 permit tcp any any eq www
58	inside	access-list acl_inside permit tcp any any eq www

Difference caused by:

NAT control in Cisco Device

Problem Source:

NAT control in Cisco devices limits access to packets which are associated with NAT rules. Thus, the source, destination addresses, or services of allowed packets are smaller than what is indicated by this Checkpoint rule.

Remedy based on allow policies:

The set of packets that are allowed in the Cisco device are shown in the Allow Policy Table. To use this table:

1. Replace this Checkpoint rule with allow rules for packets described in each row of the table.
2. Use rule reduction techniques such as address aggregation, or object grouping to reduce the number of rules to be added.

Allow Policy Table:

Service	Source	Destination
tcp/http	192.168.9.2	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

Remedy based on policy diff items:

The set of packets that are allowed by the Checkpoint device, but denied by the Cisco device, are shown in the Policy Difference Table. There may be multiple tables, each caused by a specific problem. The remedy is the following:

1. The Checkpoint rule should not be removed or altered.
2. Add rules above this Checkpoint rule to deny each packet described in the Policy Difference Table below.
3. Use rule reduction techniques such as address aggregation, or object grouping to reduce the number of rules to be added

Policy Difference Table:

Policy Diff Item	Source	Destination	Service	Cisco Rule Trails
16	192.168.9.0/24	10.0.0.0/8	tcp/http	nat:nat/Default-Deny
17	192.168.9.0/24	172.16.0.0/15	tcp/http	nat:nat/Default-Deny
18	192.168.9.0/24	192.168.2.0 to 192.168.5.255	tcp/http	nat:nat/Default-Deny
27	192.168.9.0/24	192.168.1.0/24	tcp/http	nat:nat/Default-Deny
34	192.168.9.0/24	192.168.50.0/24	tcp/http	nat:nat/Default-Deny
96	192.168.9.0/31	0.0.0.0 to 9.255.255.255	tcp/http	nat:nat/Default-Deny
97	192.168.9.0/31	11.0.0.0 to 172.15.255.255	tcp/http	nat:nat/Default-Deny
98	192.168.9.0/31	172.18.0.0 to 192.168.0.255	tcp/http	nat:nat/Default-Deny
99	192.168.9.0/31	192.168.6.0 to	tcp/http	nat:nat/Default-Deny

Policy Diff Item	Source	Destination	Service	Cisco Rule Trails
99	192.168.9.0/31	192.168.8.255	tcp/http	
100	192.168.9.0/31	192.168.10.0 to 192.168.49.255	tcp/http	nat:nat/Default-Deny
101	192.168.9.0/31	192.168.51.0 to 255.255.255.255	tcp/http	nat:nat/Default-Deny
102	192.168.9.3 to 192.168.9.255	0.0.0.0 to 9.255.255.255	tcp/http	nat:nat/Default-Deny
103	192.168.9.3 to 192.168.9.255	11.0.0.0 to 172.15.255.255	tcp/http	nat:nat/Default-Deny
104	192.168.9.3 to 192.168.9.255	172.18.0.0 to 192.168.0.255	tcp/http	nat:nat/Default-Deny
105	192.168.9.3 to 192.168.9.255	192.168.6.0 to 192.168.8.255	tcp/http	nat:nat/Default-Deny
106	192.168.9.3 to 192.168.9.255	192.168.10.0 to 192.168.49.255	tcp/http	nat:nat/Default-Deny
107	192.168.9.3 to 192.168.9.255	192.168.51.0 to 255.255.255.255	tcp/http	nat:nat/Default-Deny

Added policy caused by Checkpoint acl rule 47

Rule Index	Source	Destination	Service	VPN	Action	Comment
47	proxymail_reachable_nets	Any	https		accept	(Original ACE (line 110): access-list acl_proxymail permit tcp any any eq https)

Cisco Overlap Rules:

Line No	Interface	Rule
	vpn4	high-to-low-default-allow
103	testweb	access-list acl_testweb permit tcp any any eq https
110	proxymail	access-list acl_proxymail permit tcp any any eq https
36	outside	access-list acl_outside permit tcp any host 62.59.14.161 eq https
42	outside	access-list acl_outside permit tcp any host 62.59.14.171 eq https
51	outside	access-list acl_outside permit tcp any host 62.59.14.169 eq https
57	mail1	access-list acl_mail1 permit tcp any any eq https
59	inside	access-list acl_inside permit tcp any any eq https

Difference caused by:

NAT control in Cisco Device

Problem Source:

NAT control in Cisco devices limits access to packets which are associated with NAT rules. Thus, the source, destination addresses, or services of allowed packets are smaller than what is indicated by this Checkpoint rule.

Remedy based on allow policies:

The set of packets that are allowed in the Cisco device are shown in the Allow Policy Table. To use this table:

1. Replace this Checkpoint rule with allow rules for packets described in each row of the table.
2. Use rule reduction techniques such as address aggregation, or object grouping to reduce the number of rules to be added.

Allow Policy Table:

Service	Source	Destination
tcp/https	192.168.9.2	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

Remedy based on policy diff items:

The set of packets that are allowed by the Checkpoint device, but denied by the Cisco device, are shown in the Policy Difference Table. There may be multiple tables, each caused by a specific problem. The remedy is the following:

1. The Checkpoint rule should not be removed or altered.
2. Add rules above this Checkpoint rule to deny each packet described in the Policy Difference Table below.
3. Use rule reduction techniques such as address aggregation, or object grouping to reduce the number of rules to be added

Policy Difference Table:

Policy Diff Item	Source	Destination	Service	Cisco Rule Trails
19	192.168.9.0/24	10.0.0.0/8	tcp/https	nat:nat/Default-Deny
20	192.168.9.0/24	172.16.0.0/15	tcp/https	nat:nat/Default-Deny
21	192.168.9.0/24	192.168.2.0 to 192.168.5.255	tcp/https	nat:nat/Default-Deny
28	192.168.9.0/24	192.168.1.0/24	tcp/https	nat:nat/Default-Deny
35	192.168.9.0/24	192.168.50.0/24	tcp/https	nat:nat/Default-Deny
108	192.168.9.0/31	0.0.0.0 to 9.255.255.255	tcp/https	nat:nat/Default-Deny
109	192.168.9.0/31	11.0.0.0 to 172.15.255.255	tcp/https	nat:nat/Default-Deny
110	192.168.9.0/31	172.18.0.0 to 192.168.0.255	tcp/https	nat:nat/Default-Deny
111	192.168.9.0/31	192.168.6.0 to 192.168.8.255	tcp/https	nat:nat/Default-Deny
112	192.168.9.0/31	192.168.10.0 to 192.168.49.255	tcp/https	nat:nat/Default-Deny
113	192.168.9.0/31	192.168.51.0 to 255.255.255.255	tcp/https	nat:nat/Default-Deny
114	192.168.9.3 to 192.168.9.255	0.0.0.0 to 9.255.255.255	tcp/https	nat:nat/Default-Deny
115	192.168.9.3 to 192.168.9.255	11.0.0.0 to 172.15.255.255	tcp/https	nat:nat/Default-Deny
116	192.168.9.3 to 192.168.9.255	172.18.0.0 to 192.168.0.255	tcp/https	nat:nat/Default-Deny
117	192.168.9.3 to 192.168.9.255	192.168.6.0 to 192.168.8.255	tcp/https	nat:nat/Default-Deny
118	192.168.9.3 to 192.168.9.255	192.168.10.0 to 192.168.49.255	tcp/https	nat:nat/Default-Deny
119	192.168.9.3 to 192.168.9.255	192.168.51.0 to 255.255.255.255	tcp/https	nat:nat/Default-Deny

Added policy caused by Checkpoint acl rule 48

Rule Index	Source	Destination	Service	VPN	Action	Comment
48	proxymail_reachable_nets	Any	Migrated_sjpix_IC MP_Any		accept	(Original ACE (line 111): access-list acl_proxymail permit icmp any any)

Cisco Overlap Rules:

Line No	Interface	Rule
	vpn4	high-to-low-default-allow
107	testweb	access-list acl_testweb permit icmp any any
111	proxymail	access-list acl_proxymail permit icmp any any
50	outside	access-list acl_outside permit icmp any host 62.59.14.169
78	inside	access-list acl_inside permit icmp any any

Difference caused by:

NAT control in Cisco Device

Problem Source:

NAT control in Cisco devices limits access to packets which are associated with NAT rules. Thus, the source, destination addresses, or services of allowed packets are smaller than what is indicated by this Checkpoint rule.

Remedy based on allow policies:

The set of packets that are allowed in the Cisco device are shown in the Allow Policy Table. To use this table:

1. Replace this Checkpoint rule with allow rules for packets described in each row of the table.
2. Use rule reduction techniques such as address aggregation, or object grouping to reduce the number of rules to be added.

Allow Policy Table:

Service	Source	Destination
icmp	192.168.9.0	192.168.9.1
icmp	192.168.9.1	192.168.9.0/24
icmp	192.168.9.0 192.168.9.2 to 192.168.9.255	192.168.9.1
icmp	192.168.9.2	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

Remedy based on policy diff items:

The set of packets that are allowed by the Checkpoint device, but denied by the Cisco device, are shown in the Policy Difference Table. There may be multiple tables, each caused by a specific problem. The remedy is the following:

1. The Checkpoint rule should not be removed or altered.
2. Add rules above this Checkpoint rule to deny each packet described in the Policy Difference Table below.
3. Use rule reduction techniques such as address aggregation, or object grouping to reduce the number of rules to be added

Policy Difference Table:

Policy Diff Item	Source	Destination	Service	Cisco Rule Trails
1	192.168.9.0/24	10.0.0.0/8	icmp	nat:nat/Default-Deny
2	192.168.9.0/24	172.16.0.0/15	icmp	nat:nat/Default-Deny
3	192.168.9.0/24	192.168.2.0 to 192.168.5.255	icmp	nat:nat/Default-Deny
22	192.168.9.0/24	192.168.1.0/24	icmp	nat:nat/Default-Deny
29	192.168.9.0/24	192.168.50.0/24	icmp	nat:nat/Default-Deny
36	192.168.9.0/31	0.0.0.0 to 9.255.255.255	icmp	nat:nat/Default-Deny
41	192.168.9.0/31	11.0.0.0 to 172.15.255.255	icmp	nat:nat/Default-Deny
46	192.168.9.0/31	172.18.0.0 to 192.168.0.255	icmp	nat:nat/Default-Deny
51	192.168.9.0/31	192.168.6.0 to 192.168.8.255	icmp	nat:nat/Default-Deny
56	192.168.9.0/31	192.168.10.0 to 192.168.49.255	icmp	nat:nat/Default-Deny
61	192.168.9.0/31	192.168.51.0 to 255.255.255.255	icmp	nat:nat/Default-Deny
66	192.168.9.3 to 192.168.9.255	0.0.0.0 to 9.255.255.255	icmp	nat:nat/Default-Deny
71	192.168.9.3 to 192.168.9.255	11.0.0.0 to 172.15.255.255	icmp	nat:nat/Default-Deny
76	192.168.9.3 to 192.168.9.255	172.18.0.0 to 192.168.0.255	icmp	nat:nat/Default-Deny
81	192.168.9.3 to 192.168.9.255	192.168.6.0 to 192.168.8.255	icmp	nat:nat/Default-Deny
86	192.168.9.3 to 192.168.9.255	192.168.10.0 to 192.168.49.255	icmp	nat:nat/Default-Deny
91	192.168.9.3 to 192.168.9.255	192.168.51.0 to 255.255.255.255	icmp	nat:nat/Default-Deny

Deleted policy caused by Checkpoint acl rule 49

Rule Index	Source	Destination	Service	VPN	Action	Comment
49	proxymail_reachable_nets	Any	Any		drop	Auto-generated implied any any drop rule at end of ACL

Cisco Overlap Rules:

Line No	Interface	Rule
	any	implied-icmp-deny

Difference caused by:

ACL rules with deny action and "any" only in destination

Problem Source:

There might be two reasons for this case, which are easily identifiable from the Cisco acl match/overlap rule table above:

1. Improper translation

There is no matching rule, but there are overlap rules: source or service field may be an incorrect translation. If policy difference-based remedy proposed below results in a large number of added rules, an alternative remedy is to correct the incorrectly translated field, if that can be identified. You might have to run this report again to ensure that the fix is complete.

2. Zone spanning

Here is an exact match with a Cisco rule, yet the Cisco rule may have its source include networks that are not reachable from the corresponding interface. They are harmless in the Cisco context but can cause additional allow or deny policies in Checkpoint.

Remedy:

Identify the source addresses that are specified in this Checkpoint rule and that are part of the reachable networks in the reachability table. Replace the source address in this Checkpoint rule with only those source addresses.

Refer to [Cisco Reachability Table](#)

Remedy based on policy diff items:

The set of packets that are denied by the Checkpoint device, but allowed by the Cisco device, are shown in the Policy Difference Table. There may be multiple tables, each caused by a specific problem. The remedy is the following:

1. The Checkpoint rule should not be removed or altered.
2. Add rules above this Checkpoint rule to allow packets described in each row of the Policy Difference Table below.
3. Use rule reduction techniques such as address aggregation, or object grouping to reduce the number of rules to be added

Policy Difference Table:

Policy Diff Item	Source	Destination	Service	Cisco Rule Trails
120	192.168.9.2	0.0.0.0 to 9.255.255.255	icmp	acl:111
125	192.168.9.2	11.0.0.0 to 172.15.255.255	icmp	acl:111
130	192.168.9.2	172.18.0.0 to 192.168.0.255	icmp	acl:111
135	192.168.9.2	192.168.6.0 to 192.168.8.255	icmp	acl:111
140	192.168.9.2	192.168.10.0 to 192.168.49.255	icmp	acl:111
145	192.168.9.2	192.168.51.0 to 255.255.255.255	icmp	acl:111

Added policy caused by Checkpoint acl rule 50

Rule Index	Source	Destination	Service	VPN	Action	Comment
50	testweb_reachable_nets	Any	http		accept	(Original ACE (line 102): access-list acl_testweb permit tcp any any eq www)

Cisco Overlap Rules:

Line No	Interface	Rule
	vpn4	high-to-low-default-allow
102	testweb	access-list acl_testweb permit tcp any any eq www
109	proxymail	access-list acl_proxymail permit tcp any any eq www
35	outside	access-list acl_outside permit tcp any host 62.59.14.161 eq www
40	outside	access-list acl_outside permit tcp any host 62.59.14.170 eq www
41	outside	access-list acl_outside permit tcp any host 62.59.14.171 eq www
52	outside	access-list acl_outside permit tcp any host 62.59.14.169 eq www
56	mail1	access-list acl_mail1 permit tcp any any eq www
58	inside	access-list acl_inside permit tcp any any eq www

Difference caused by:

NAT control in Cisco Device

Problem Source:

NAT control in Cisco devices limits access to packets which are associated with NAT rules. Thus, the source, destination addresses, or services of allowed packets are smaller than what is indicated by this Checkpoint rule.

Remedy based on allow policies:

The set of packets that are allowed in the Cisco device are shown in the Allow Policy Table. To use this table:

1. Replace this Checkpoint rule with allow rules for packets described in each row of the table.
2. Use rule reduction techniques such as address aggregation, or object grouping to reduce the number of rules to be added.

Allow Policy Table:

Service	Source	Destination
tcp/http	192.168.50.0/24	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

Remedy based on policy diff items:

The set of packets that are allowed by the Checkpoint device, but denied by the Cisco device, are shown in the Policy Difference Table. There may be multiple tables, each caused by a specific problem. The remedy is the following:

1. The Checkpoint rule should not be removed or altered.
2. Add rules above this Checkpoint rule to deny each packet described in the Policy Difference Table below.
3. Use rule reduction techniques such as address aggregation, or object grouping to reduce the number of rules to be added

Policy Difference Table:

Policy Diff Item	Source	Destination	Service	Cisco Rule Trails
448	192.168.50.0/24	192.168.9.0/24	tcp/http	nat:nat/Default-Deny
473	192.168.50.0/24	10.0.0.0/8	tcp/http	nat:nat/Default-Deny
474	192.168.50.0/24	172.16.0.0/15	tcp/http	nat:nat/Default-Deny
475	192.168.50.0/24	192.168.2.0 to 192.168.5.255	tcp/http	nat:nat/Default-Deny
492	192.168.50.0/24	192.168.1.0/24	tcp/http	nat:nat/Default-Deny

Added policy caused by Checkpoint acl rule 51

Rule Index	Source	Destination	Service	VPN	Action	Comment
51	testweb_reachable_nets	Any	https		accept	(Original ACE (line 103): access-list acl_testweb permit tcp any any eq https)

Cisco Overlap Rules:

Line No	Interface	Rule
	vpn4	high-to-low-default-allow
103	testweb	access-list acl_testweb permit tcp any any eq https
110	proxymail	access-list acl_proxymail permit tcp any any eq https
36	outside	access-list acl_outside permit tcp any host 62.59.14.161 eq https
42	outside	access-list acl_outside permit tcp any host 62.59.14.171 eq https

Line No	Interface	Rule
51	outside	access-list acl_outside permit tcp any host 62.59.14.169 eq https
57	mail1	access-list acl_mail1 permit tcp any any eq https
59	inside	access-list acl_inside permit tcp any any eq https

Difference caused by:

NAT control in Cisco Device

Problem Source:

NAT control in Cisco devices limits access to packets which are associated with NAT rules. Thus, the source, destination addresses, or services of allowed packets are smaller than what is indicated by this Checkpoint rule.

Remedy based on allow policies:

The set of packets that are allowed in the Cisco device are shown in the Allow Policy Table. To use this table:

1. Replace this Checkpoint rule with allow rules for packets described in each row of the table.
2. Use rule reduction techniques such as address aggregation, or object grouping to reduce the number of rules to be added.

Allow Policy Table:

Service	Source	Destination
tcp/https	192.168.50.0/24	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

Remedy based on policy diff items:

The set of packets that are allowed by the Checkpoint device, but denied by the Cisco device, are shown in the Policy Difference Table. There may be multiple tables, each caused by a specific problem. The remedy is the following:

1. The Checkpoint rule should not be removed or altered.
2. Add rules above this Checkpoint rule to deny each packet described in the Policy Difference Table below.
3. Use rule reduction techniques such as address aggregation, or object grouping to reduce the number of rules to be added

Policy Difference Table:

Policy Diff Item	Source	Destination	Service	Cisco Rule Trails
449	192.168.50.0/24	192.168.9.0/24	tcp/https	nat:nat/Default-Deny
476	192.168.50.0/24	10.0.0.0/8	tcp/https	nat:nat/Default-Deny
477	192.168.50.0/24	172.16.0.0/15	tcp/https	nat:nat/Default-Deny
478	192.168.50.0/24	192.168.2.0 to 192.168.5.255	tcp/https	nat:nat/Default-Deny

Policy Diff Item	Source	Destination	Service	Cisco Rule Trails
493	192.168.50.0/24	192.168.1.0/24	tcp/https	nat:nat/Default-Deny

Added policy caused by Checkpoint acl rule 52

Rule Index	Source	Destination	Service	VPN	Action	Comment
52	testweb_reachable_nets	Any	ssh		accept	(Original ACE (line 104): access-list acl_testweb permit tcp any any eq ssh)

Cisco Overlap Rules:

Line No	Interface	Rule
	vpn4	high-to-low-default-allow
104	testweb	access-list acl_testweb permit tcp any any eq ssh
43	outside	access-list acl_outside permit tcp any host 62.59.14.171 eq ssh
64	inside	access-list acl_inside permit tcp any any eq ssh

Difference caused by:

NAT control in Cisco Device

Problem Source:

NAT control in Cisco devices limits access to packets which are associated with NAT rules. Thus, the source, destination addresses, or services of allowed packets are smaller than what is indicated by this Checkpoint rule.

Remedy based on allow policies:

The set of packets that are allowed in the Cisco device are shown in the Allow Policy Table. To use this table:

1. Replace this Checkpoint rule with allow rules for packets described in each row of the table.
2. Use rule reduction techniques such as address aggregation, or object grouping to reduce the number of rules to be added.

Allow Policy Table:

Service	Source	Destination
tcp/ssh	192.168.50.0/24	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

Remedy based on policy diff items:

The set of packets that are allowed by the Checkpoint device, but denied by the Cisco device, are shown in the Policy Difference Table. There may be multiple tables, each caused by a specific problem. The remedy is the following:

1. The Checkpoint rule should not be removed or altered.
2. Add rules above this Checkpoint rule to deny each packet described in the Policy Difference Table below.
3. Use rule reduction techniques such as address aggregation, or object grouping to reduce the number of rules to be added

Policy Difference Table:

Policy Diff Item	Source	Destination	Service	Cisco Rule Trails
446	192.168.50.0/24	192.168.9.0/24	tcp/ssh	nat:nat/Default-Deny
467	192.168.50.0/24	10.0.0.0/8	tcp/ssh	nat:nat/Default-Deny
468	192.168.50.0/24	172.16.0.0/15	tcp/ssh	nat:nat/Default-Deny
469	192.168.50.0/24	192.168.2.0 to 192.168.5.255	tcp/ssh	nat:nat/Default-Deny
490	192.168.50.0/24	192.168.1.0/24	tcp/ssh	nat:nat/Default-Deny

Added policy caused by Checkpoint acl rule 53

Rule Index	Source	Destination	Service	VPN	Action	Comment
53	testweb_reachable_nets	Any	smtp		accept	(Original ACE (line 105): access-list acl_testweb permit tcp any any eq smtp)

Cisco Overlap Rules:

Line No	Interface	Rule
	vpn4	high-to-low-default-allow
105	testweb	access-list acl_testweb permit tcp any any eq smtp
53	mail1	access-list acl_mail1 permit tcp any host 192.168.1.4 eq smtp

Difference caused by:

NAT control in Cisco Device

Problem Source:

NAT control in Cisco devices limits access to packets which are associated with NAT rules. Thus, the source, destination addresses, or services of allowed packets are smaller than what is indicated by this Checkpoint rule.

Remedy based on allow policies:

The set of packets that are allowed in the Cisco device are shown in the Allow Policy Table. To use this table:

1. Replace this Checkpoint rule with allow rules for packets described in each row of the table.
2. Use rule reduction techniques such as address aggregation, or object grouping to reduce the number of rules to be added.

Allow Policy Table:

Service	Source	Destination
tcp/smtp	192.168.50.0/24	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

Remedy based on policy diff items:

The set of packets that are allowed by the Checkpoint device, but denied by the Cisco device, are shown in the Policy Difference Table. There may be multiple tables, each caused by a specific problem. The remedy is the following:

1. The Checkpoint rule should not be removed or altered.
2. Add rules above this Checkpoint rule to deny each packet described in the Policy Difference Table below.
3. Use rule reduction techniques such as address aggregation, or object grouping to reduce the number of rules to be added

Policy Difference Table:

Policy Diff Item	Source	Destination	Service	Cisco Rule Trails
447	192.168.50.0/24	192.168.9.0/24	tcp/smtp	nat:nat/Default-Deny
470	192.168.50.0/24	10.0.0.0/8	tcp/smtp	nat:nat/Default-Deny
471	192.168.50.0/24	172.16.0.0/15	tcp/smtp	nat:nat/Default-Deny
472	192.168.50.0/24	192.168.2.0 to 192.168.5.255	tcp/smtp	nat:nat/Default-Deny
491	192.168.50.0/24	192.168.1.0/24	tcp/smtp	nat:nat/Default-Deny

Added policy caused by Checkpoint acl rule 54

Rule Index	Source	Destination	Service	VPN	Action	Comment
54	testweb_reachable_nets	Any	Migrated_UDP_Service_195		accept	(Original ACE (line 106): access-list acl_testweb permit udp any any eq dnsix)

Cisco Overlap Rules:

Line No	Interface	Rule
	vpn4	high-to-low-default-allow
91	inside	access-list acl_inside permit udp any any

Difference caused by:

ACL rules with allow action and "any" only in destination

Problem Source:

Device architecture difference allows more packets in the Checkpoint device than the equivalent rule in the Cisco device. Another cause may be the absence of an equivalent Cisco rule.

Remedy:

Add deny rules in front of this Checkpoint rule to deny the policy items listed below.

Remedy based on policy diff items:

The set of packets that are allowed by the Checkpoint device, but denied by the Cisco device, are shown in the Policy Difference Table. There may be multiple tables, each caused by a specific problem. The remedy is the following:

1. The Checkpoint rule should not be removed or altered.
2. Add rules above this Checkpoint rule to deny each packet described in the Policy Difference Table below.
3. Use rule reduction techniques such as address aggregation, or object grouping to reduce the number of rules to be added.

Policy Difference Table:

Policy Diff Item	Source	Destination	Service	Cisco Rule Trails
451	192.168.50.0/24	192.168.9.0/24	udp/dn6-nlm-aud	acl:access-list-acl_testweb- implied-deny
482	192.168.50.0/24	10.0.0.0/8	udp/dn6-nlm-aud	acl:access-list-acl_testweb- implied-deny
483	192.168.50.0/24	172.16.0.0/15	udp/dn6-nlm-aud	acl:access-list-acl_testweb- implied-deny
484	192.168.50.0/24	192.168.2.0 to 192.168.5.255	udp/dn6-nlm-aud	acl:access-list-acl_testweb- implied-deny
495	192.168.50.0/24	192.168.1.0/24	udp/dn6-nlm-aud	acl:access-list-acl_testweb- implied-deny
496	192.168.50.0/24	0.0.0.0 to 9.255.255.255	udp/dn6-nlm-aud	acl:access-list-acl_testweb- implied-deny
497	192.168.50.0/24	11.0.0.0 to 172.15.255.255	udp/dn6-nlm-aud	acl:access-list-acl_testweb- implied-deny
498	192.168.50.0/24	172.18.0.0 to 192.168.0.255	udp/dn6-nlm-aud	acl:access-list-acl_testweb- implied-deny
499	192.168.50.0/24	192.168.6.0 to 192.168.8.255	udp/dn6-nlm-aud	acl:access-list-acl_testweb- implied-deny
500	192.168.50.0/24	192.168.10.0 to 192.168.49.255	udp/dn6-nlm-aud	acl:access-list-acl_testweb- implied-deny
501	192.168.50.0/24	192.168.51.0 to 255.255.255.255	udp/dn6-nlm-aud	acl:access-list-acl_testweb- implied-deny

Added policy caused by Checkpoint acl rule 55

Rule Index	Source	Destination	Service	VPN	Action	Comment
55	testweb_reachable_nets	Any	Migrated_sjpix_IC MP_Any		accept	(Original ACE (line 107): access-list acl_testweb permit icmp any any)

Cisco Overlap Rules:

Line No	Interface	Rule
	vpn4	high-to-low-default-allow
107	testweb	access-list acl_testweb permit icmp any any
111	proxymail	access-list acl_proxymail permit icmp any any
50	outside	access-list acl_outside permit icmp any host 62.59.14.169
78	inside	access-list acl_inside permit icmp any any

Difference caused by:

NAT control in Cisco Device

Problem Source:

NAT control in Cisco devices limits access to packets which are associated with NAT rules. Thus, the source, destination addresses, or services of allowed packets are smaller than what is indicated by this Checkpoint rule.

Remedy based on allow policies:

The set of packets that are allowed in the Cisco device are shown in the Allow Policy Table. To use this table:

1. Replace this Checkpoint rule with allow rules for packets described in each row of the table.
2. Use rule reduction techniques such as address aggregation, or object grouping to reduce the number of rules to be added.

Allow Policy Table:

Service	Source	Destination
icmp	192.168.50.0/24	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
icmp	192.168.50.1	192.168.10.0 to 255.255.255.255
icmp	192.168.50.0 192.168.50.2 to 192.168.50.255	192.168.10.0 to 192.168.49.255 192.168.50.1 192.168.51.0 to 255.255.255.255

Remedy based on policy diff items:

The set of packets that are allowed by the Checkpoint device, but denied by the Cisco device, are shown in the Policy Difference Table. There may be multiple tables, each caused by a specific problem. The remedy is the following:

1. The Checkpoint rule should not be removed or altered.

2. Add rules above this Checkpoint rule to deny each packet described in the Policy Difference Table below.
3. Use rule reduction techniques such as address aggregation, or object grouping to reduce the number of rules to be added

Policy Difference Table:

Policy Diff Item	Source	Destination	Service	Cisco Rule Trails
441	192.168.50.0/24	192.168.9.0/24	icmp	nat:nat/Default-Deny
452	192.168.50.0/24	10.0.0.0/8	icmp	nat:nat/Default-Deny
453	192.168.50.0/24	172.16.0.0/15	icmp	nat:nat/Default-Deny
454	192.168.50.0/24	192.168.2.0 to 192.168.5.255	icmp	nat:nat/Default-Deny
485	192.168.50.0/24	192.168.1.0/24	icmp	nat:nat/Default-Deny

Added policy caused by Checkpoint acl rule 56

Rule Index	Source	Destination	Service	VPN	Action	Comment
56	testweb_reachable_nets	Any	domain-udp		accept	(Original ACE (line 108): access-list acl_testweb permit udp any any eq domain)

Cisco Overlap Rules:

Line No	Interface	Rule
	vpn4	high-to-low-default-allow
108	testweb	access-list acl_testweb permit udp any any eq domain
91	inside	access-list acl_inside permit udp any any

Difference caused by:

NAT control in Cisco Device

Problem Source:

NAT control in Cisco devices limits access to packets which are associated with NAT rules. Thus, the source, destination addresses, or services of allowed packets are smaller than what is indicated by this Checkpoint rule.

Remedy based on allow policies:

The set of packets that are allowed in the Cisco device are shown in the Allow Policy Table. To use this table:

1. Replace this Checkpoint rule with allow rules for packets described in each row of the table.
2. Use rule reduction techniques such as address aggregation, or object grouping to reduce the number of rules to be added.

Allow Policy Table:

Service	Source	Destination
udp/domain	192.168.50.0/24	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

Remedy based on policy diff items:

The set of packets that are allowed by the Checkpoint device, but denied by the Cisco device, are shown in the Policy Difference Table. There may be multiple tables, each caused by a specific problem. The remedy is the following:

1. The Checkpoint rule should not be removed or altered.
2. Add rules above this Checkpoint rule to deny each packet described in the Policy Difference Table below.
3. Use rule reduction techniques such as address aggregation, or object grouping to reduce the number of rules to be added

Policy Difference Table:

Policy Diff Item	Source	Destination	Service	Cisco Rule Trails
450	192.168.50.0/24	192.168.9.0/24	udp/domain	nat:nat/Default-Deny
479	192.168.50.0/24	10.0.0.0/8	udp/domain	nat:nat/Default-Deny
480	192.168.50.0/24	172.16.0.0/15	udp/domain	nat:nat/Default-Deny
481	192.168.50.0/24	192.168.2.0 to 192.168.5.255	udp/domain	nat:nat/Default-Deny
494	192.168.50.0/24	192.168.1.0/24	udp/domain	nat:nat/Default-Deny

Deleted policy caused by Checkpoint acl rule 57

Rule Index	Source	Destination	Service	VPN	Action	Comment
57	testweb_reachable_nets	Any	Any		drop	Auto-generated implied any any drop rule at end of ACL

Cisco Overlap Rules:

Line No	Interface	Rule
	any	implied-icmp-deny

Difference caused by:

ACL rules with deny action and "any" only in destination

Problem Source:

There might be two reasons for this case, which are easily identifiable from the Cisco acl match/overlap rule table above:

1. Improper translation
There is no matching rule, but there are overlap rules: source or service field may be an incorrect translation. If policy difference-based remedy proposed below results in a large number of added rules, an alternative remedy is to correct the incorrectly translated field, if that can be identified. You might have to run this report again to ensure that the fix is complete.
2. Zone spanning
Here is an exact match with a Cisco rule, yet the Cisco rule may have its source include networks that are not reachable from the corresponding interface. They are harmless in the Cisco context but can cause additional allow or deny policies in Checkpoint.

Remedy:

Identify the source addresses that are specified in this Checkpoint rule and that are part of the reachable networks in the reachability table. Replace the source address in this Checkpoint rule with only those source addresses.

Refer to [Cisco Reachability Table](#)

Remedy based on policy diff items:

The set of packets that are denied by the Checkpoint device, but allowed by the Cisco device, are shown in the Policy Difference Table. There may be multiple tables, each caused by a specific problem. The remedy is the following:

1. The Checkpoint rule should not be removed or altered.
2. Add rules above this Checkpoint rule to allow packets described in each row of the Policy Difference Table below.
3. Use rule reduction techniques such as address aggregation, or object grouping to reduce the number of rules to be added

Policy Difference Table:

Policy Diff Item	Source	Destination	Service	Cisco Rule Trails
502	192.168.50.0/24	0.0.0.0 to 9.255.255.255	icmp	acl:107
507	192.168.50.0/24	11.0.0.0 to 172.15.255.255	icmp	acl:107
512	192.168.50.0/24	172.18.0.0 to 192.168.0.255	icmp	acl:107
517	192.168.50.0/24	192.168.6.0 to 192.168.8.255	icmp	acl:107
522	192.168.50.0/24	192.168.10.0 to 192.168.49.255	icmp	acl:107
527	192.168.50.0/24	192.168.51.0 to 255.255.255.255	icmp	acl:107
532	192.168.50.0/24	0.0.0.0 to 9.255.255.255	udp/dnsix	acl:106
533	192.168.50.0/24	11.0.0.0 to 172.15.255.255	udp/dnsix	acl:106
534	192.168.50.0/24	172.18.0.0 to 192.168.0.255	udp/dnsix	acl:106
535	192.168.50.0/24	192.168.6.0 to 192.168.8.255	udp/dnsix	acl:106
536	192.168.50.0/24	192.168.10.0 to 192.168.49.255	udp/dnsix	acl:106
537	192.168.50.0/24	192.168.51.0 to 255.255.255.255	udp/dnsix	acl:106

Deleted policy caused by Checkpoint acl rule 76

Rule Index	Source	Destination	Service	VPN	Action	Comment
76	Migrated_sjpix_outside_Interface	Any	Any		drop	Auto-generated implied any any drop rule at end of ACL

Cisco Overlap Rules:

Line No	Interface	Rule
	any	implied-icmp-deny

Difference caused by:

ACL rules with deny action and "any" only in destination

Problem Source:

There might be two reasons for this case, which are easily identifiable from the Cisco acl match/overlap rule table above:

1. Improper translation

There is no matching rule, but there are overlap rules: source or service field may be an incorrect translation. If policy difference-based remedy proposed below results in a large number of added rules, an alternative remedy is to correct the incorrectly translated field, if that can be identified. You might have to run this report again to ensure that the fix is complete.

2. Zone spanning

Here is an exact match with a Cisco rule, yet the Cisco rule may have its source include networks that are not reachable from the corresponding interface. They are harmless in the Cisco context but can cause additional allow or deny policies in Checkpoint.

Remedy:

Identify the source addresses that are specified in this Checkpoint rule and that are part of the reachable networks in the reachability table. Replace the source address in this Checkpoint rule with only those source addresses.

Refer to [Cisco Reachability Table](#)

Remedy based on policy diff items:

The set of packets that are denied by the Checkpoint device, but allowed by the Cisco device, are shown in the Policy Difference Table. There may be multiple tables, each caused by a specific problem. The remedy is the following:

1. The Checkpoint rule should not be removed or altered.
2. Add rules above this Checkpoint rule to allow packets described in each row of the Policy Difference Table below.
3. Use rule reduction techniques such as address aggregation, or object grouping to reduce the number of rules to be added

Policy Difference Table:

Policy Diff Item	Source	Destination	Service	Cisco Rule Trails
541	62.59.14.160/27	62.59.14.169	icmp	acl:50

Deleted policy caused by Checkpoint acl rule 77

Rule Index	Source	Destination	Service	VPN	Action	Comment
77	Any	Any	Any		drop	Auto-generated global cleanup rule (not a part of the original configuration)

Difference caused by:

ACL clean up rule

Problem Source:

Improperly translated or missed acl allow rule.

Remedy:

See remedy based on policy diff items.

Remedy based on policy diff items:

The set of packets that are denied by the Checkpoint device, but allowed by the Cisco device, are shown in the Policy Difference Table. There may be multiple tables, each caused by a specific problem. The remedy is the following:

1. Add rules at the beginning of Checkpoint security ruleset to allow each packet described in the Policy Difference Table below.
2. Use rule reduction techniques such as address aggregation, or object grouping to reduce the number of rules to be added.

Policy Difference Table:

Policy Diff Item	Source	Destination	Service	Cisco Rule Trails
539	0.0.0.0 to 9.255.255.255	62.59.14.169	icmp	acl:50
540	11.0.0.0 to 62.59.14.159	62.59.14.169	icmp	acl:50
546	127.0.0.2 to 172.15.255.255	62.59.14.169	icmp	acl:50
546	62.59.14.192 to 127.0.0.0	62.59.14.169	icmp	acl:50

Policy Diff Item	Source	Destination	Service	Cisco Rule Trails
547	172.18.0.0 to 192.168.0.255	62.59.14.169	icmp	acl:50
548	192.168.6.0 to 192.168.8.255	62.59.14.169	icmp	acl:50
549	192.168.10.0 to 192.168.49.255	62.59.14.169	icmp	acl:50
550	192.168.51.0 to 255.255.255.255	62.59.14.169	icmp	acl:50
551	0.0.0.0 to 9.255.255.255	62.59.14.161	tcp/http	acl:35
552	0.0.0.0 to 9.255.255.255	62.59.14.169	tcp/http	acl:52
553	11.0.0.0 to 62.59.14.159	62.59.14.161	tcp/http	acl:35
554	11.0.0.0 to 62.59.14.159	62.59.14.169	tcp/http	acl:52
555	127.0.0.2 to 172.15.255.255	62.59.14.161	tcp/http	acl:35
555	62.59.14.192 to 127.0.0.0	62.59.14.161	tcp/http	acl:35
556	127.0.0.2 to 172.15.255.255	62.59.14.169	tcp/http	acl:52
556	62.59.14.192 to 127.0.0.0	62.59.14.169	tcp/http	acl:52
557	172.18.0.0 to 192.168.0.255	62.59.14.161	tcp/http	acl:35
558	172.18.0.0 to 192.168.0.255	62.59.14.169	tcp/http	acl:52
559	192.168.6.0 to 192.168.8.255	62.59.14.161	tcp/http	acl:35
560	192.168.6.0 to 192.168.8.255	62.59.14.169	tcp/http	acl:52
561	192.168.10.0 to 192.168.49.255	62.59.14.161	tcp/http	acl:35
562	192.168.10.0 to 192.168.49.255	62.59.14.169	tcp/http	acl:52
563	192.168.51.0 to 255.255.255.255	62.59.14.161	tcp/http	acl:35
564	192.168.51.0 to 255.255.255.255	62.59.14.169	tcp/http	acl:52
565	0.0.0.0 to 9.255.255.255	62.59.14.161	tcp/https	acl:36
566	0.0.0.0 to 9.255.255.255	62.59.14.169	tcp/https	acl:51
567	11.0.0.0 to 62.59.14.159	62.59.14.161	tcp/https	acl:36
568	11.0.0.0 to 62.59.14.159	62.59.14.169	tcp/https	acl:51
569	62.59.14.192 to 127.0.0.0	62.59.14.161	tcp/https	acl:36
569	127.0.0.2 to 172.15.255.255	62.59.14.161	tcp/https	acl:36
570	127.0.0.2 to 172.15.255.255	62.59.14.169	tcp/https	acl:51
570	62.59.14.192 to 127.0.0.0	62.59.14.169	tcp/https	acl:51
571	172.18.0.0 to 192.168.0.255	62.59.14.161	tcp/https	acl:36
572	172.18.0.0 to 192.168.0.255	62.59.14.169	tcp/https	acl:51
573	192.168.6.0 to 192.168.8.255	62.59.14.161	tcp/https	acl:36
574	192.168.6.0 to 192.168.8.255	62.59.14.169	tcp/https	acl:51
575	192.168.10.0 to 192.168.49.255	62.59.14.161	tcp/https	acl:36
576	192.168.10.0 to 192.168.49.255	62.59.14.169	tcp/https	acl:51
577	192.168.51.0 to 255.255.255.255	62.59.14.161	tcp/https	acl:36
578	192.168.51.0 to 255.255.255.255	62.59.14.169	tcp/https	acl:51
589	0.0.0.0 to 9.255.255.255	62.59.14.171	tcp/ssh	acl:43
590	11.0.0.0 to 62.59.14.159	62.59.14.171	tcp/ssh	acl:43

Policy Diff Item	Source	Destination	Service	Cisco Rule Trails
591	62.59.14.192 to 127.0.0.0	62.59.14.171	tcp/ssh	acl:43
591	127.0.0.2 to 172.15.255.255	62.59.14.171	tcp/ssh	acl:43
592	172.18.0.0 to 192.168.0.255	62.59.14.171	tcp/ssh	acl:43
593	192.168.6.0 to 192.168.8.255	62.59.14.171	tcp/ssh	acl:43
594	192.168.10.0 to 192.168.49.255	62.59.14.171	tcp/ssh	acl:43
595	192.168.51.0 to 255.255.255.255	62.59.14.171	tcp/ssh	acl:43
596	0.0.0.0 to 9.255.255.255	62.59.14.171	tcp/http	acl:41
597	11.0.0.0 to 62.59.14.159	62.59.14.171	tcp/http	acl:41
598	127.0.0.2 to 172.15.255.255	62.59.14.171	tcp/http	acl:41
598	62.59.14.192 to 127.0.0.0	62.59.14.171	tcp/http	acl:41
599	172.18.0.0 to 192.168.0.255	62.59.14.171	tcp/http	acl:41
600	192.168.6.0 to 192.168.8.255	62.59.14.171	tcp/http	acl:41
601	192.168.10.0 to 192.168.49.255	62.59.14.171	tcp/http	acl:41
602	192.168.51.0 to 255.255.255.255	62.59.14.171	tcp/http	acl:41
603	0.0.0.0 to 9.255.255.255	62.59.14.171	tcp/https	acl:42
604	11.0.0.0 to 62.59.14.159	62.59.14.171	tcp/https	acl:42
605	127.0.0.2 to 172.15.255.255	62.59.14.171	tcp/https	acl:42
605	62.59.14.192 to 127.0.0.0	62.59.14.171	tcp/https	acl:42
606	172.18.0.0 to 192.168.0.255	62.59.14.171	tcp/https	acl:42
607	192.168.6.0 to 192.168.8.255	62.59.14.171	tcp/https	acl:42
608	192.168.10.0 to 192.168.49.255	62.59.14.171	tcp/https	acl:42
609	192.168.51.0 to 255.255.255.255	62.59.14.171	tcp/https	acl:42

Checkpoint Device NAT Table

Source	Destination	Service	Translated Source	Translated Destination	Translated Service
172.16.0.0/16	192.168.16.0/24	any	original	original	original
10.0.0.0/8	192.168.16.0/24	any	original	original	original
192.168.16.0/24	172.16.0.0/16	any	original	original	original
192.168.16.0/24	10.0.0.0/8	any	original	original	original
192.168.1.0/24	192.168.1.4	any	original	172.16.0.19	original
172.16.0.19	192.168.1.0/24	any	192.168.1.4	original	original
192.168.2.0/24	192.168.50.0/24	any	192.168.50.5	original	original
192.168.3.0/24	192.168.50.0/24	any	192.168.50.4	original	original
172.16.0.0/16	192.168.1.0/24	any	192.168.1.3	original	original
172.16.0.0/16	192.168.50.0/24	any	192.168.50.3	original	original
172.17.0.0/16	192.168.50.0/24	any	192.168.50.6	original	original
10.0.0.0/8	192.168.50.0/24	any	192.168.50.6	original	original

Source	Destination	Service	Translated Source	Translated Destination	Translated Service
192.168.1.0/24	192.168.50.0/24	any	192.168.50.3	original	original
192.168.1.2	any	any	62.59.14.163	original	original
192.168.50.2	any	any	62.59.14.171	original	original
192.168.9.2	any	any	62.59.14.169	original	original
192.168.9.2	any	any	62.59.14.161	original	original
192.168.2.0/24	any	any	62.59.14.167	original	original
192.168.3.0/24	any	any	62.59.14.164	original	original
192.168.4.0/24	any	any	62.59.14.165	original	original
192.168.5.0/24	any	any	62.59.14.166	original	original
172.16.0.0/16	any	any	62.59.14.162	original	original
172.17.0.0/16	any	any	62.59.14.168	original	original
10.0.0.0/8	any	any	62.59.14.168	original	original
192.168.1.0/24	any	any	62.59.14.162	original	original
192.168.50.0/24	any	any	62.59.14.162	original	original
any	62.59.14.163	any	original	192.168.1.2	original
any	62.59.14.171	any	original	192.168.50.2	original
any	62.59.14.169	any	original	192.168.9.2	original
any	62.59.14.161	any	original	192.168.9.2	original

Cisco Device Reachability Table

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

Checkpoint Device Reachability Table

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
	mail1 (192.168.1.1/255.255.255.0)	192.168.1.0/24
	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
	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

Policies from Cisco Device

This section lists destination addresses that are the origin of all IP services that are allowed to connect from the firewall device itself. The list of allowed services is grouped by each interface from which the IP traffic leaves the firewall.

Exiting Interface	Service	Dst Address
inside (172.16.0.1/255.255.0.0)	icmp	10.0.0.0/8
		172.16.0.0/15
		192.168.2.0 to 192.168.5.255
	udp/snmptrap	172.16.0.61
udp/rsh	172.16.0.200	
mail1 (192.168.1.1/255.255.255.0)	icmp	192.168.1.0/24
outside (62.59.14.189/255.255.255.224)	icmp	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
proxymail (192.168.9.1/255.255.255.0)	icmp	192.168.9.0/24
testweb (192.168.50.1/255.255.255.0)	icmp	192.168.50.0/24

Policies to Cisco Device

This section lists source addresses that are the origin of all IP services that are allowed to connect to the firewall device itself. The list of services is grouped by each interface to which the IP traffic enters the firewall.

Entering Interface	Service	Src Address
inside (172.16.0.1/255.255.0.0)	icmp	10.0.0.0/8
		172.16.0.0/15
		192.168.2.0 to 192.168.5.255
	tcp/telnet	172.16.0.0/16
		192.168.3.0/24
	tcp/https	172.16.0.101
		172.16.0.200
		172.16.6.44
		172.16.31.46
	udp/snmp	172.16.0.61
mail1 (192.168.1.1/255.255.255.0)	icmp	192.168.1.0/24
outside (62.59.14.189/255.255.255.224)	icmp	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
proxymail (192.168.9.1/255.255.255.0)	icmp	192.168.9.0/24
testweb (192.168.50.1/255.255.255.0)	icmp	192.168.50.0/24