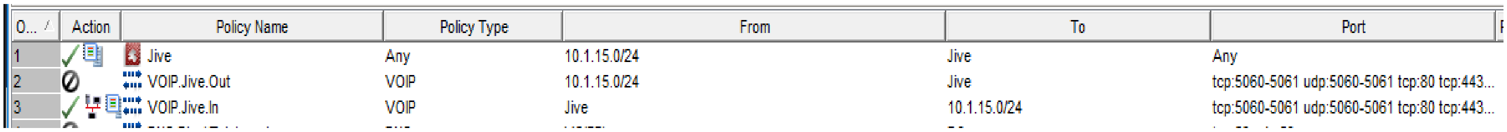
QPC Analysis On Jive VOIP Services

DO NOT MAKE YOUR POLICY THIS WAY. THIS IS WRONG.
QPC did not create this configuration. It is an example of what NOT to do.



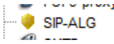
O...	Action	Policy Name	Policy Type	From	To	Port
1	✓	Jive	Any	10.1.15.0/24	Jive	Any
2	⊘	VOIP.Jive.Out	VOIP	10.1.15.0/24	Jive	tcp:5060-5061 udp:5060-5061 tcp:80 tcp:443...
3	✓	VOIP.Jive.In	VOIP	Jive	10.1.15.0/24	tcp:5060-5061 udp:5060-5061 tcp:80 tcp:443...

Policy 1 does absolutely nothing. Egress traffic was fully allowed previously. There was never anything in the logs showing egress traffic being blocked.
This is an example of opening a hole for no reason.

Never hard code subnets into **From** or **To** areas of a policy. This will cause the policy to break when the subnet definition changes elsewhere.
Only the Voice VLAN alias should be used there.
The **VOIP.Jive.Out** policy should not be disabled. There was no evidence that any packets outbound were being blocked. An any policy is a very bad choice from a security perspective.
Also note that if your related policies do not all have the same string in their title (such as VOIP), you will not have efficient traffic searching.
This is another failing of policy 1.

There should be a single policy that is **Jive.In.Out** with Policy Type VOIP. The source and destinations (From/To) should have the Voice VLAN and Jive alias in there so that ingress and egress traffic can flow between those destinations.
If Jive had a decent service, this configuration would not be necessary.

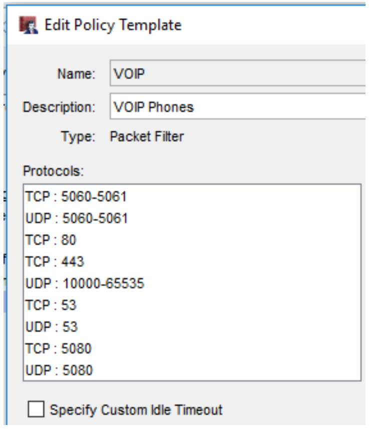
In fact, Jives service worked exclusively with Policy 2 for months. Then one day unannounced, they changed their cloud server configuration without informing customers.
The end result is that customers had service outages.
And when Jive support was contacted, they claimed, as they always do, that a SIP-ALG was in use. No SIP-ALG was in use and it never had been.
A SIP-ALG looks like this.



SIP-ALG

So if you don't see a yellow shield and there is no policy type specified as SIP-ALG, there is no SIP-ALG. It's that simple. Jive … please do everyone a favor and stop claiming that there is a SIP-ALG when there is not. When a customer's phone service works for months, and it suddenly stops working when there were no security appliance changes, a SIP-ALG did not just suddenly appear.

Here is our custom port collection for the Jive VOIP phones. In Firebox, this is called Policy.
We think this is a really bad name because the policies actually show up in the screens where you see the full From/To information.
Instead, these should be called port collections. They are collections of ports and protocols as a packet filter. Nothing more. They do not make a policy.
You can see that the entire high dynamic range of UDP ports is included because apparently Jive cannot manage to make their service work over a reasonable range such as 5060 - 5062.
Port 53 is so that the phones can use Internet DNS servers to find the Jive servers.



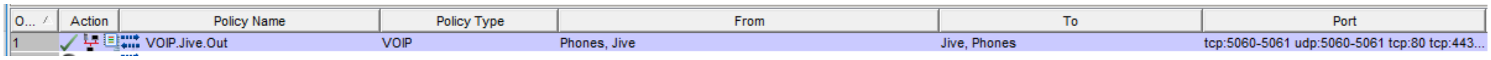
Edit Policy Template

Name: VOIP
Description: VOIP Phones
Type: Packet Filter

Protocols:
TCP : 5060-5061
UDP : 5060-5061
TCP : 80
TCP : 443
UDP : 10000-65535
TCP : 53
UDP : 53
TCP : 5080
UDP : 5080

□ Specify Custom Idle Timeout

This is what we would recommend for making Jive services work without compromising security.
You see that there is no technical limitation that requires a single From or To. You can use this technique to make an elegant bi-directional policy and to accommodate their flawed session handling.
Also note that logging and traffic management are enabled. Traffic management is a QoS bandwidth floor guarantee.



O...	Action	Policy Name	Policy Type	From	To	Port
1	✓	VOIP.Jive.Out	VOIP	Phones, Jive	Jive, Phones	tcp:5060-5061 udp:5060-5061 tcp:80 tcp:443...

VOIP is an alias for a completely isolated VLAN that can do nothing but talk to the Jive servers on the Internet and publicly available DNS servers.
And where Jive is an alias for a set of IP subnets that are part of Jives's network.