

How to Configure VOIP Connections with the Skinny (SCCP) Firewall Plugin

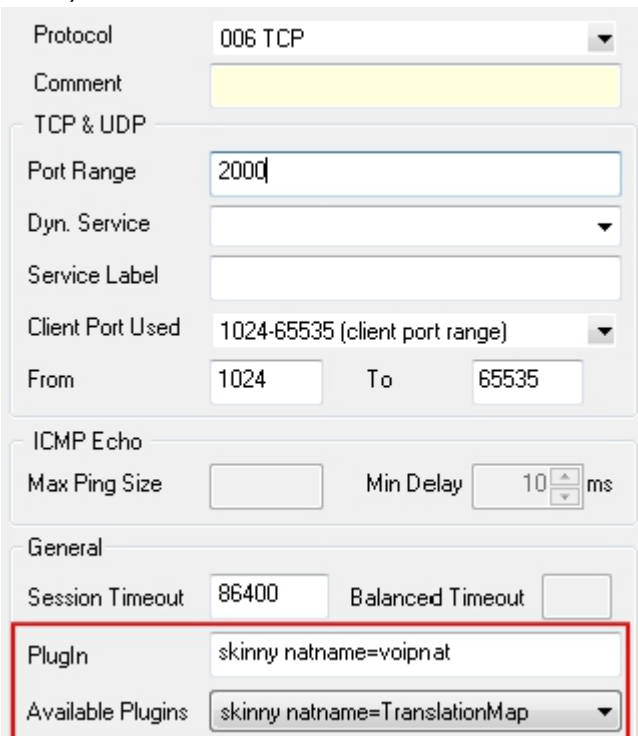
<https://campus.barracuda.com/doc/48203072/>

SCCP (Skinny Client Control Protocol) is the protocol used by Cisco callmanager software for VOIP telephony. The VOIP connection is made up out of two separate connections: the control connection handling signaling and RTP data streams for the audio/video transmissions. In order to open the necessary dynamic ports for the RTP connection you need to use the Skinny firewall plugin. The plugin monitors the signaling connection between the VOIP phone and the Cisco callmanager on TCP port 2000. When a new call is initiated the plugin will interpret the packet containing the connection information and open the ports. Similarly these ports are closed when the plugin detects the corresponding call release packet in the skinny control connection.

Step 1. Create Service Objects for Signalling and Streaming Purpose

For information concerning service objects, see [How to Create Service Objects](#). The skinny plugin has two optional parameters which can be entered in the **Plugin** field:

- **natname** - is a reference to a Network Address Translation Map in the **Connections** tab in the firewall rule set (syntax: *skinny natname=*) and handles the signalling (protocol: *TCP*, port: *2000*).



Protocol: 006 TCP

Comment: [Empty]

TCP & UDP

Port Range: 2000

Dyn. Service: [Empty]

Service Label: [Empty]

Client Port Used: 1024-65535 (client port range)

From: 1024 To: 65535

ICMP Echo

Max Ping Size: [Empty] Min Delay: 10 ms

General

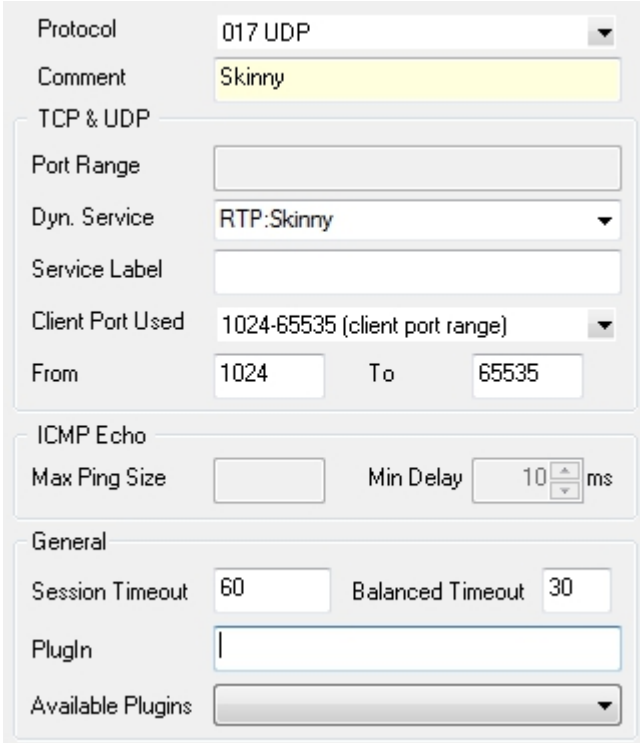
Session Timeout: 86400 Balanced Timeout: [Empty]

Plugin: **skinny natname=voipnat**

Available Plugins: **skinny natname=TranslationMap**

If this option is not specified then the default value *RTP:Skinny* (see below) is used instead. No address translation is performed for the RTP media streams if there is no matching entry in **Connections**.

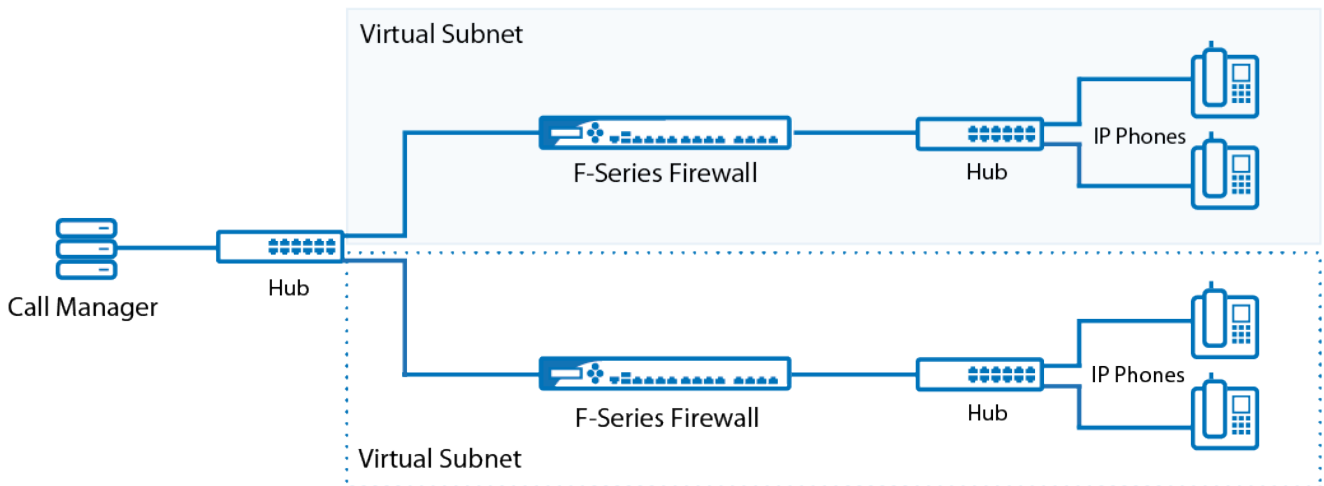
- **srvname** - is a reference to a Dyn. Service label that data fills a service object with the data stream of skinny calls (syntax: *skinny [srvname=]*) (protocol: *UDP*). The service object can be referenced by a firewall rule in order to forward the media streams between the call participants. The default value of *srvname* is *RTP:Skinny*.



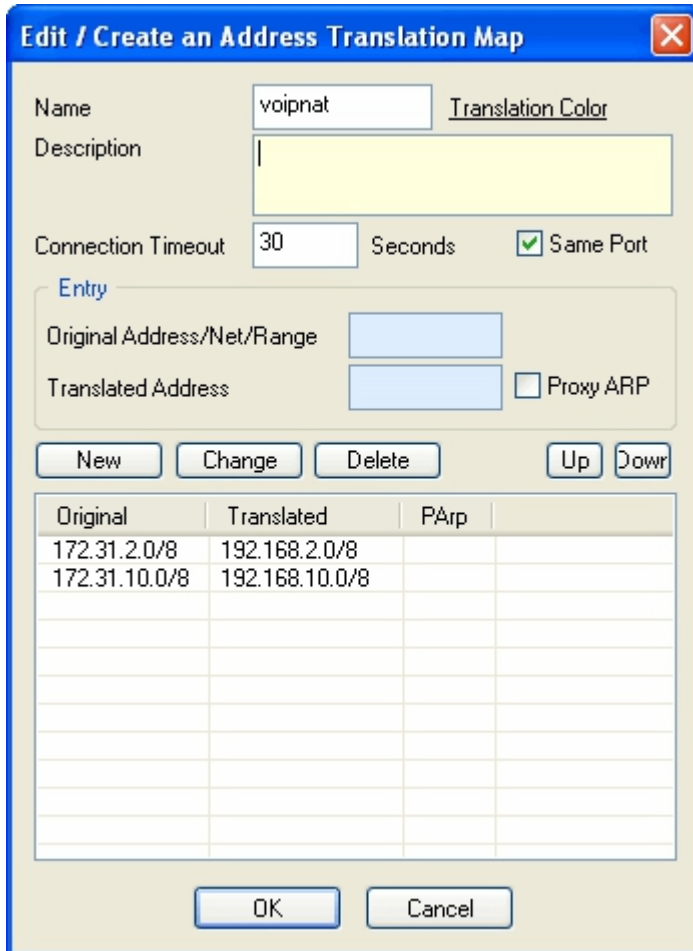
The screenshot shows the configuration for a service object. The 'Protocol' is set to '017 UDP'. The 'Comment' is 'Skinny'. Under the 'TCP & UDP' section, 'Port Range' is empty, 'Dyn. Service' is 'RTP:Skinny', 'Service Label' is empty, and 'Client Port Used' is '1024-65535 (client port range)'. The 'From' port is '1024' and the 'To' port is '65535'. Under the 'ICMP Echo' section, 'Max Ping Size' is empty and 'Min Delay' is '10 ms'. Under the 'General' section, 'Session Timeout' is '60' and 'Balanced Timeout' is '30'. There is an empty 'Plugin' field and an 'Available Plugins' dropdown menu.

Step 2. Create Translation Map (optional)

If network address translation is done between caller and callee an address translation map has to be defined, translating the real IP address of the participants to virtual addresses that are routeable for all nodes in the VOIP network. For more information, see [How to Create NAT Tables \(Translation Maps\)](#).



The name of the map must match the option of the **natname** parameter of the skinny firewall plugin configured above. The Original Address/Net is the physical IP subnet of a node whereas the Translated Address/Net is the virtual address.



Edit / Create an Address Translation Map

Name: voipnat Translation Color

Description:

Connection Timeout: 30 Seconds Same Port

Entry

Original Address/Net/Range:

Translated Address: Proxy ARP

New Change Delete Up Down

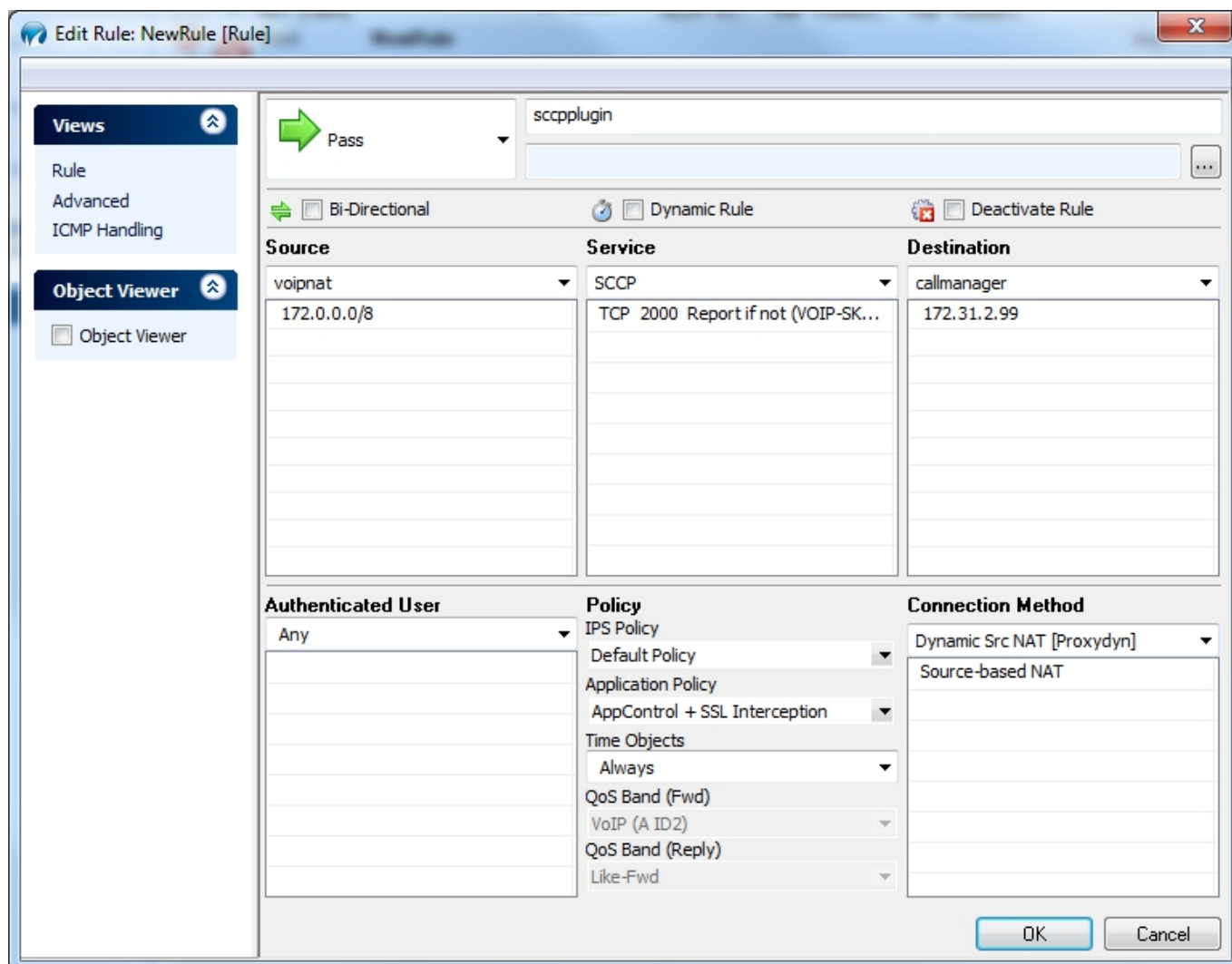
Original	Translated	PArp
172.31.2.0/8	192.168.2.0/8	
172.31.10.0/8	192.168.10.0/8	

OK Cancel

In a call setup message the real address of the phone is translated to the virtual address. As soon as the other participant of the call receives the modified call setup message it starts sending its voice stream to the virtual address of the peer. The firewall next to the receiver of the media stream re-translates the virtual IP address back to the real address of the participant.

The firewall rule required for proper address translation handling has to contain a reference to the service object with the *RTP Dyn*. Service label specified in the skinny plugin (see above). The mapping rule action controls how the address mapping is performed. To use the same address map which is used by the skinny plugin, select the same map in the **Redirection** and **Source Translation** section. If no address translation is required then the [Pass](#) firewall action is to be used.

Skinny signal protocol firewall rule with Skinny firewall plugin:



RTP firewall rule with network address translation from the voipnat address translation map:

Edit Rule: NewRule [Rule]
X

Views ⬆

- Rule
- Advanced
- ICMP Handling

Object Viewer ⬆

Object Viewer

➡ Map

Bi-Directional
 Dynamic Rule
 Deactivate Rule

Source	Service	Destination
<div style="margin-bottom: 5px;">World</div> <div style="border: 1px solid #ccc; padding: 2px;">0.0.0.0/0</div>	<div style="margin-bottom: 5px;">RTP</div> <div style="border: 1px solid #ccc; padding: 2px;">UDP RTP:Skinny Report if not (V...</div>	<div style="margin-bottom: 5px;">voipnat</div> <div style="border: 1px solid #ccc; padding: 2px;">Mapped IP/Mask</div>
<div style="margin-bottom: 5px;">Authenticated User</div> <div style="border: 1px solid #ccc; padding: 2px;">Any</div>	<div style="margin-bottom: 5px;">Policy</div> <div style="border: 1px solid #ccc; padding: 2px;"> IPS Policy Default Policy Application Policy AppControl + SSL Interception Time Objects Always QoS Band (Fwd) VoIP (A ID2) QoS Band (Reply) Like-Fwd </div>	<div style="margin-bottom: 5px;">Connection Method</div> <div style="border: 1px solid #ccc; padding: 2px;">voipnat</div>

OK

Cancel

Figures

1. skinny_tcp.jpg
2. skinny_srv.jpg
3. voip_skinny.png
4. transl_fw.jpg
5. sccp_plugin_new.jpg
6. rtp_map_new.jpg

© Barracuda Networks Inc., 2019 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.