



Configuration Guide

for

**Sipera UC-Sec 1U and UC-Sec 2U
Version: 3.7**

with

**Nortel Communication Server 2100
SE11**

**Issue 1.0
July 2009**

**Sipera Systems
1900 Firman Drive
Suite 600
Richardson, TX 75081**

Table of Contents

Table of Contents	2
Objective	3
UC-Sec SIP Trunking Overview	3
UC-Sec SIP Remote User/ Line-Side Overview	3
Configuration Steps (SIP Trunk)	4
Step 1: IP Addresses	4
Step 2: Signaling Interfaces	5
Step 3: Media Interfaces	6
Step 4: Topology Hiding Profile for Line-side CS 2100	7
Step 5: Topology Hiding Profile for Trunk-side CS 2100.....	8
Step 6: Routing Profile for Line-side CS 2100.....	9
Step 7: Routing Profile for Trunk-side CS 2100	10
Step 8: CS 2100 Interworking Profile – General Tab.....	11
Step 9: CS 2100 Interworking Profile – Advanced Tab	12
Step 10: Server Configuration for Line-side CS 2100 – General	13
Step 11: Server Configuration for Line-side CS 2100 – Advanced.....	14
Step 12: Server Configuration for Trunk-side CS 2100 - General	15
Step 13: Server Configuration for Trunk-side CS 2100 - Advanced.....	16
Step 14: Server Flows for Line-side CS 2100	17
Step 15: Server Flows for Trunk-side CS 2100.....	18
Configuration Steps (SIP Line-Side)	19
Step 1: IP Addresses	19
Step 2: Signaling Interfaces	20
Step 3: Media Interfaces	21
Step 4: Topology Hiding Profile (Phone side).....	22
Step 5: Topology Hiding Profile (Server side)	23
Step 6: Routing Profile (Phone side)	24
Step 7: Routing Profile (Server side).....	25
Step 8: CS 2100 Interworking Profile – General Tab.....	26
Step 9: CS 2100 Interworking Profile – Advanced Tab	27
Step 10: Server configuration	28
Step 11: Server Configuration for Line-side CS 2100 – Advanced.....	29
Step 12: End Point Policy Group	30
Step 13: Subscriber Flows	31
Step 14: Subscriber Flows(cont'd).....	32
Step 15: Server Flows	33

Objective

The aim of this document is to provide guidelines for configuring UC-Sec 1U and UC-Sec 2U in a SIP trunking and SIP line-side deployment scenario, interoperating with Nortel Communication Server 2100 (CS 2100) platforms on both the line-side and the trunk-side.

UC-Sec SIP Trunking Overview

The Sipera UC-Sec SIP Trunking solution provides connectivity to IP private branch exchanges (IP PBXs). The SIP trunk provides direct access to the customer premise-based IP PBX via SIP signaling, and complements the existing features of the IP PBX. The SIP trunk architecture has the following components-

- Line-side IP-PBX (CS 2100) provides the call control, call capacity, voice mail, etc.
- Sipera UC-Sec is the SBC which hides the network topology, providing network security and the demarcation point between the remote call server and the peer/enterprise call server.
- Trunk-side IP-PBX (CS 2100) provides call routing and phone service at the remote site.

UC-Sec SIP Remote User/ Line-Side Overview

The remote user solution from Sipera Systems allows enterprises to extend the VoIP and unified communications functions of their IP PBX over the Internet to remote IP phones, soft phones and WiFi/dual-mode phones. Built on the foundation of the Sipera VIPER engine and real-time platform, the UC-Sec appliances perform the following functions in a SIP Remote user deployment scenario:

- protect against threats by blocking them at the enterprise perimeter
- offer fine-grained policy enforcement based on user, network, device and time of day
- integrate with AAA and two-factor authentication servers for strong access control
- serve as the termination point for encrypted TLS and SRTP streams traversing the uncontrolled Internet
- simplify the deployment of mobile workspaces by providing firewall/NAT traversal security, phone configuration proxy, and preservation of voice QoS

Configuration Steps (SIP Trunk)

Step 1: IP Addresses

Goto “Device Specific Settings” → “Network Management” → “Network Configuration”

Configure the IP addresses, subnet mask and the default gateways for the network interfaces on UC-Sec. This step requires the configuration of a minimum of two IP addresses, one for communication between UC-Sec and the line-side CS 2100, and the other for communication between UC-Sec and the trunk-side CS 2100. The two IP addresses, if on the same subnet, can be configured on the same network interface (single-wire mode). If the IP addresses are on different subnets, they must be configured on two separate network interfaces (two-wire mode).

For the trunking configuration in ‘Enterprise NAT’ mode, the Public IP on the B1 interface (interfacing to the trunk-side CS 2100) must be configured as the enterprise NAT’s public IP. In a ‘No NAT’ deployment scenario the Public IP configuration is not needed.

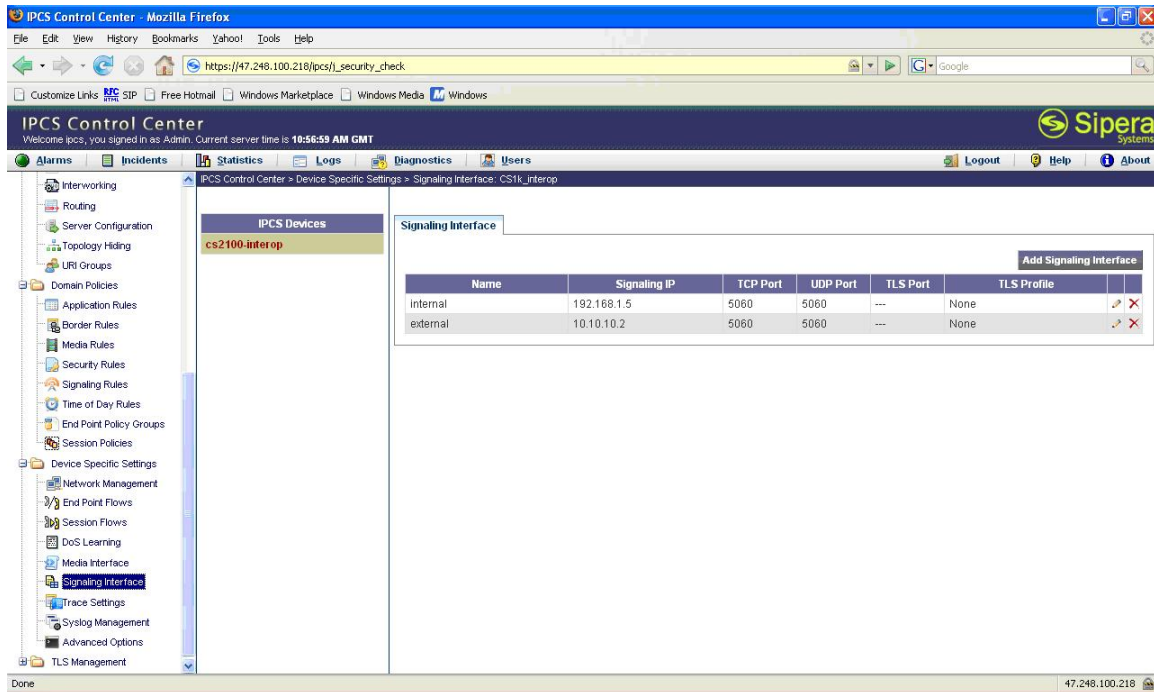
The screenshot shows the IPCS Control Center web interface in a Mozilla Firefox browser. The URL is https://47.249.100.218/ipcs/_security_check. The interface is for the 'IPCS Control Center' and shows the user is signed in as 'Admin'. The current server time is 10:56:25 AM GMT. The left sidebar contains a tree view with categories like Alarms, Incidents, Statistics, Logs, Diagnostics, Users, and Device Specific Settings. The 'Device Specific Settings' category is expanded, showing 'Network Management' as the selected option. The main content area is titled 'IPCS Devices' and shows a list of devices, with 'cs2100.interop' selected. The 'Network Configuration' tab is active, displaying a form for configuring network settings. The form includes fields for A1 Netmask (255.255.255.0), A2 Netmask, B1 Netmask (255.255.255.0), and B2 Netmask. Below these fields is a table for adding IP addresses. The table has columns for IP Address, Public IP, Gateway, and Interface. Two rows are shown: one for interface A1 with IP 192.168.1.5 and gateway 192.168.1.1, and another for interface B1 with IP 10.10.10.2 and gateway 10.10.10.1. The status bar at the bottom shows 'Done' and the IP address 47.249.100.218.

IP Address	Public IP	Gateway	Interface
192.168.1.5		192.168.1.1	A1
10.10.10.2	47.249.100.66	10.10.10.1	B1

Step 2: Signaling Interfaces

Goto “Device Specific Settings” → “Signalling Interface” → “Add Signaling Interface”

The signaling interfaces for the IP addresses already configured on the UC-Sec must be configured with the transport protocol supported on each interface. This will be used for signaling to a logical name, which will later be tied to Server flows.



The screenshot shows the IPCS Control Center web interface in a Mozilla Firefox browser. The address bar displays `https://47.248.100.218/ipcs/_security_check`. The interface includes a navigation menu on the left with categories like Interworking, Routing, Server Configuration, and Device Specific Settings. The 'Device Specific Settings' category is expanded, showing 'Signaling Interface' as the selected option. The main content area is titled 'IPCS Control Center > Device Specific Settings > Signaling Interface: CS1k_interop'. It features a table with two signaling interfaces: 'internal' and 'external'. The 'internal' interface has a Signaling IP of 192.168.1.5, TCP Port of 5060, UDP Port of 5060, and TLS Port of ---. The 'external' interface has a Signaling IP of 10.10.10.2, TCP Port of 5060, UDP Port of 5060, and TLS Port of ---. Both interfaces have a TLS Profile of 'None'. An 'Add Signaling Interface' button is located at the top right of the table.

Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile
internal	192.168.1.5	5060	5060	---	None
external	10.10.10.2	5060	5060	---	None

Step 3: Media Interfaces

Goto “Device Specific Settings” → “Media Interface” → “Add Media Interface”

The media interfaces for the IP addresses already configured on the UC-Sec must be configured to assign a logical name to the port ranges used for RTP. This will be tied to Server flows.

The screenshot shows the IPCS Control Center web interface in a Mozilla Firefox browser. The address bar shows the URL https://47.249.100.218/ipcs/_security_check. The interface is titled "IPCS Control Center" and shows the user is signed in as Admin. The current server time is 10:57:22 AM GMT. The left sidebar contains a tree view of configuration options, including "Device Specific Settings" which is expanded to show "Media Interface". The main content area displays the "Media Interface" configuration for the device "cs2100.interop". It includes a table with columns "Name", "Media IP", and "Port Range". The table contains two entries: "internal" with Media IP 192.168.1.5 and Port Range 35000 - 40000, and "external" with Media IP 10.10.10.2 and Port Range 35000 - 40000. There is an "Add Media Interface" button in the top right corner of the table.

Name	Media IP	Port Range
internal	192.168.1.5	35000 - 40000
external	10.10.10.2	35000 - 40000

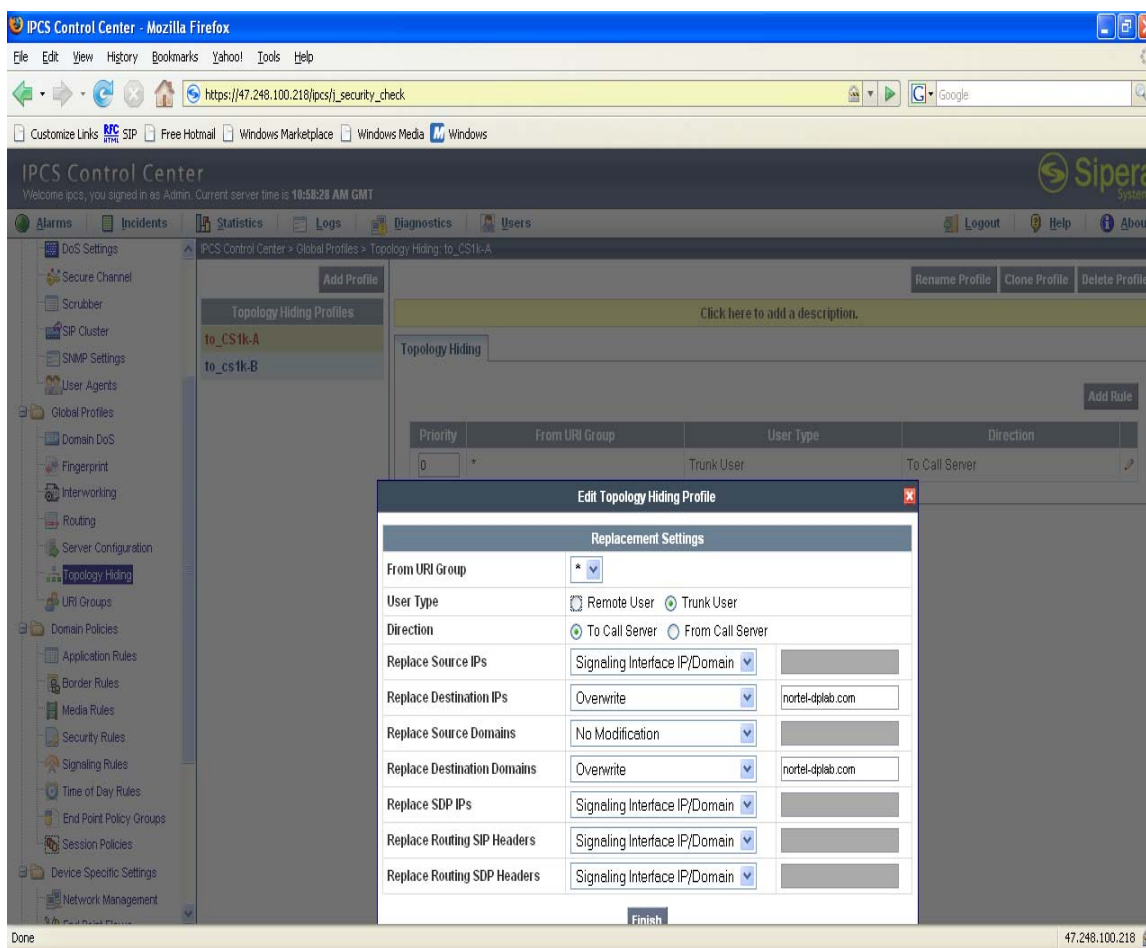
Step 4: Topology Hiding Profile for Line-side CS 2100

Goto “Global Profiles” → “Topology Hiding” → “Add Topology Hiding Profile”

Topology Hiding profiles must be configured with the following options:

- user type defined as ‘Trunk user’,
- direction defined as ‘To Call Server’

As a result of this configuration, the action taken by the topology hiding feature occurs when UC-Sec is ready to send the SIP message to the call server. The action to be taken by the ‘topology hiding’ feature in both SIP and SDP headers is selected from the drop down menu, as shown in the screen below. The topology hiding profile must be configured for both the line-side and trunk-side CS 2100 servers. The screen below shows the profile configuration for the line-side server.

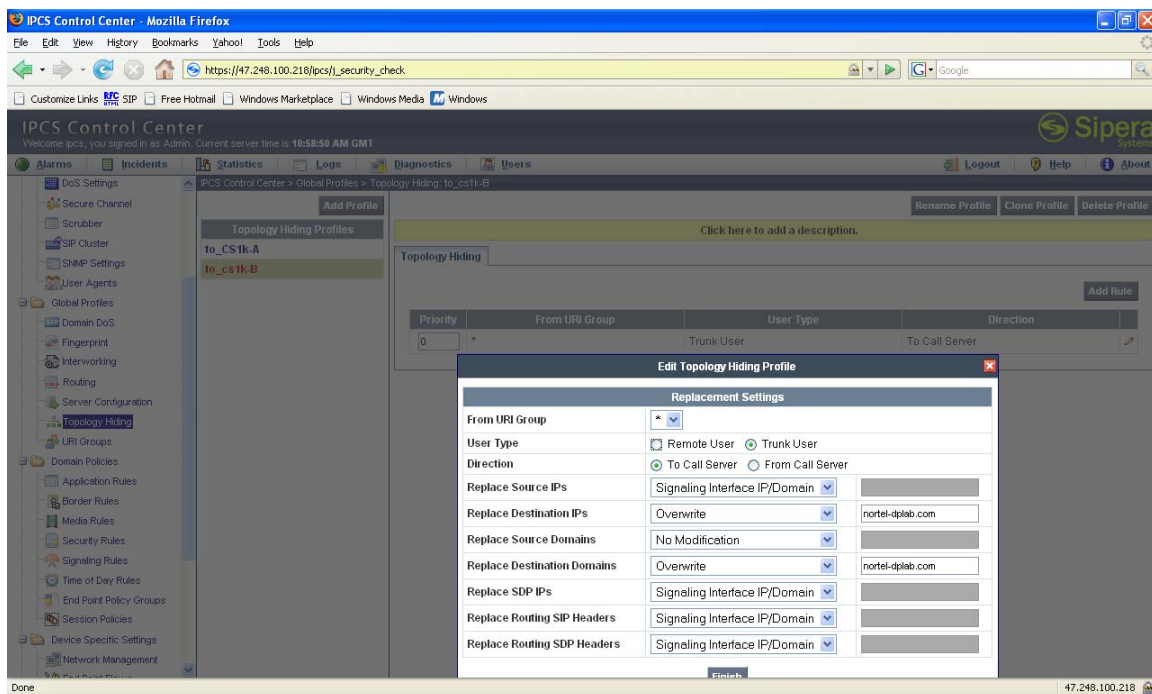


Step 5: Topology Hiding Profile for Trunk-side CS 2100

Goto “Global Profiles” → “Topology Hiding” → “Add Topology Hiding Profile”

Topology Hiding profiles must be configured with the following options:
 user type defined as ‘Trunk user’,
 direction defined as ‘To Call Server’.

As a result of this configuration, the action taken by the topology hiding feature occurs when UC-Sec is ready to send the SIP message to the call server. The action to be taken by the topology hiding feature in both SIP and SDP headers is selected from the drop down menu as shown in the screen below. The topology hiding profile must be configured for both the line-side and trunk-side CS 2100 servers. The screen below shows the profile configuration for the trunk-side server.



Step 6: Routing Profile for Line-side CS 2100

Goto 'Global Profiles' → 'Routing' → 'Add Profile'

Routing profiles define where SIP packets will be routed when the profile is used in a 'Server Configuration'. The routing can either be 'Next Hop Server'-based or based on DNS (NAPTR, SRV) lookups. The configuration provided below is 'Next Hop Server'-based. This profile is used in the server configuration for 'CS 2100-B', which means that any SIP packets originating from the trunk-side server will be routed to the identified IP address, which is the line-side server.

The screenshot shows the IPCS Control Center web interface in a Mozilla Firefox browser. The address bar shows the URL https://47.248.100.218/ipcs/_security_check. The interface includes a sidebar with navigation options like Alarms, Incidents, Statistics, Logs, Diagnostics, and Users. The main content area displays the 'Routing Profiles' section, where a new profile named 'cs2100-B' is being added. The profile configuration includes a table for routing rules.

Priority	URI Group	Next Hop Server 1	Next Hop Server 2	NAPTR	SRV	Outgoing Transport
1	*	192.168.1.9	---	<input type="checkbox"/>	<input type="checkbox"/>	UDP

Step 7: Routing Profile for Trunk-side CS 2100

Goto 'Global Profiles' → 'Routing' → 'Add Profile'

Routing profiles define where SIP packets will be routed when the profile is called in a 'Server Configuration'. The routing can either be 'Next Hop Server'-based, or based on DNS (NAPTR, SRV) lookups. The configuration provided below is 'Next Hop Server'-based. This profile is used in the server configuration 'CS 2100-A', which means that any SIP packets originating from the line-side server will be routed to the identified IP address, which is the trunk-side server.

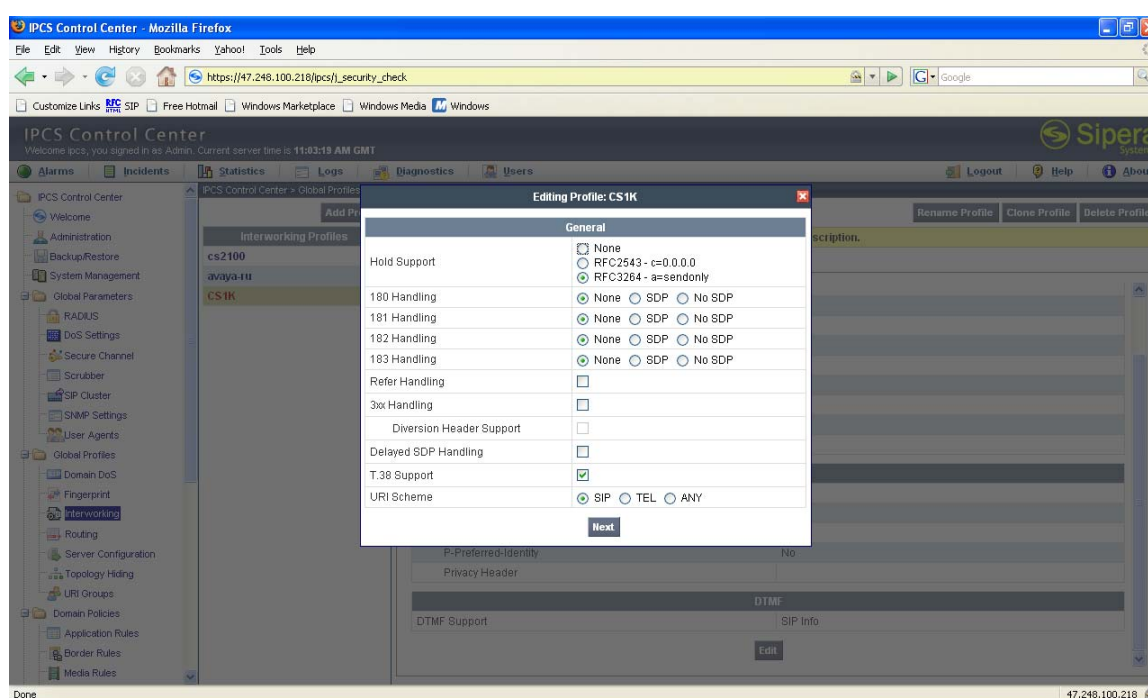
The screenshot shows the IPCS Control Center web interface in Mozilla Firefox. The browser address bar shows the URL https://47.248.100.218/ipcs/_security_check. The interface includes a sidebar with navigation options such as 'Alarms', 'Incidents', 'Statistics', 'Logs', 'Diagnostics', 'Users', 'Logout', 'Help', and 'About'. The main content area is titled 'Routing Profiles' and shows a list of profiles: 'default', 'cs2100-A', and 'cs2100-B'. The 'cs2100-B' profile is selected, and its configuration details are displayed. The configuration includes a table for 'All available URI groups are used in this Routing Profile.' with the following data:

Priority	URI Group	Next Hop Server 1	Next Hop Server 2	NAPTR	SRV	Outgoing Transport
1	*	47.248.100.226	---	<input type="checkbox"/>	<input type="checkbox"/>	UDP

Step 8: CS 2100 Interworking Profile – General Tab

Goto ‘Global Profiles’ → ‘Interworking’ → ‘Add Profile’

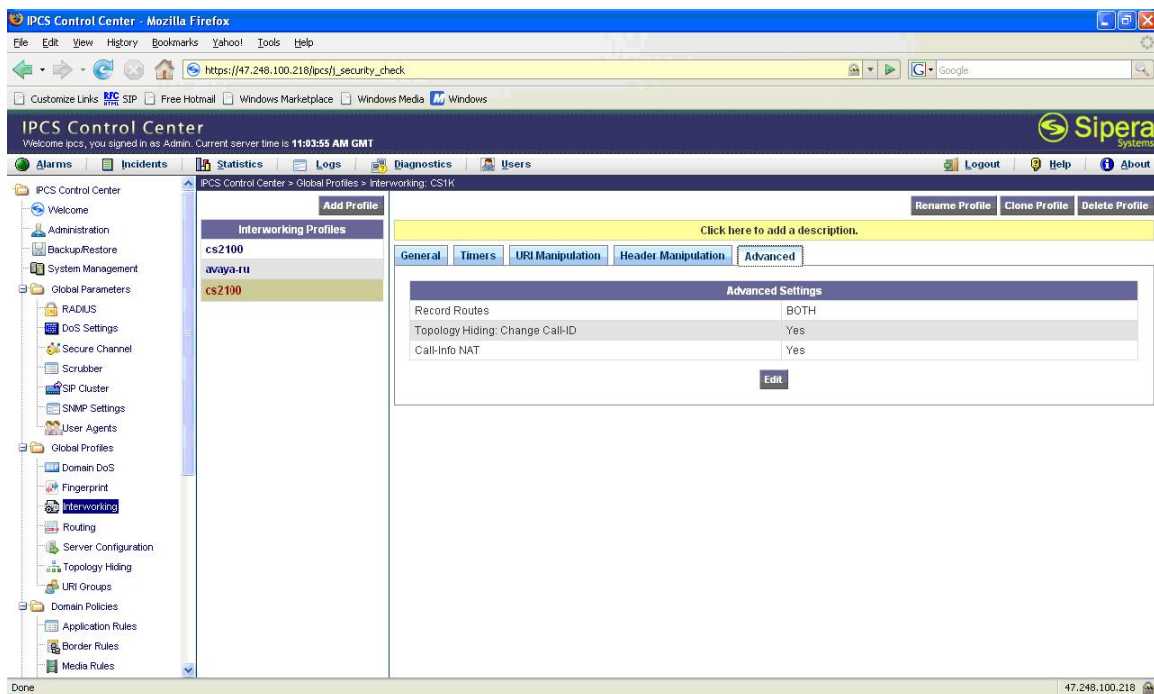
Interworking profiles improve interoperability by enabling communication between servers from different vendors. An interworking profile for CS 2100 is provided below. This profile defines the message handling by UC-Sec for various messages when communicating to a CS 2100. The profile will be linked to the ‘Server Configuration’. The following screen shows the configuration under the ‘General’ tab in the ‘Interworking Profile’ for CS 2100.



Step 9: CS 2100 Interworking Profile – Advanced Tab

Goto ‘Global Profiles’ → ‘Interworking’ → ‘Add Profile’

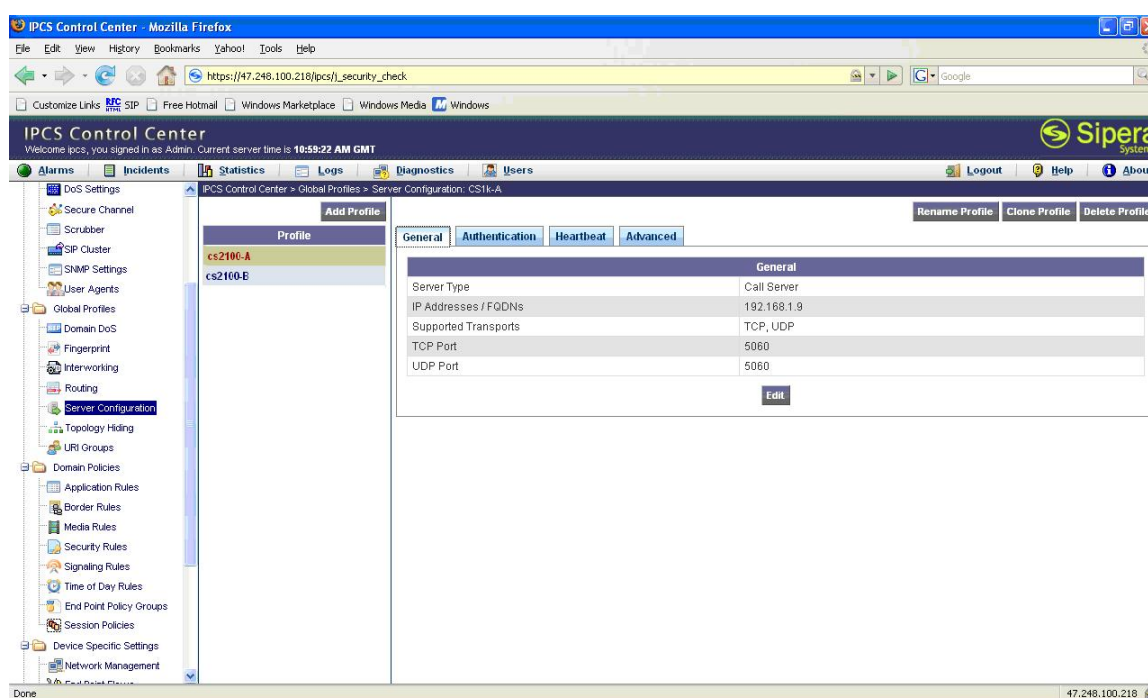
Interworking profiles improve interoperability by enabling communication between servers from different vendors. An interworking profile for CS 2100 is provided below. This profile defines the message handling by UC-Sec for various messages when communicating to a CS 2100. This profile will be linked to the ‘Server Configuration’. The following screen shows the configuration under the ‘Advanced’ tab in the ‘Interworking Profile’ for CS 2100.



Step 10: Server Configuration for Line-side CS 2100 – General

Goto “Global Profiles” → “Server Configuration” → “Add Profile”

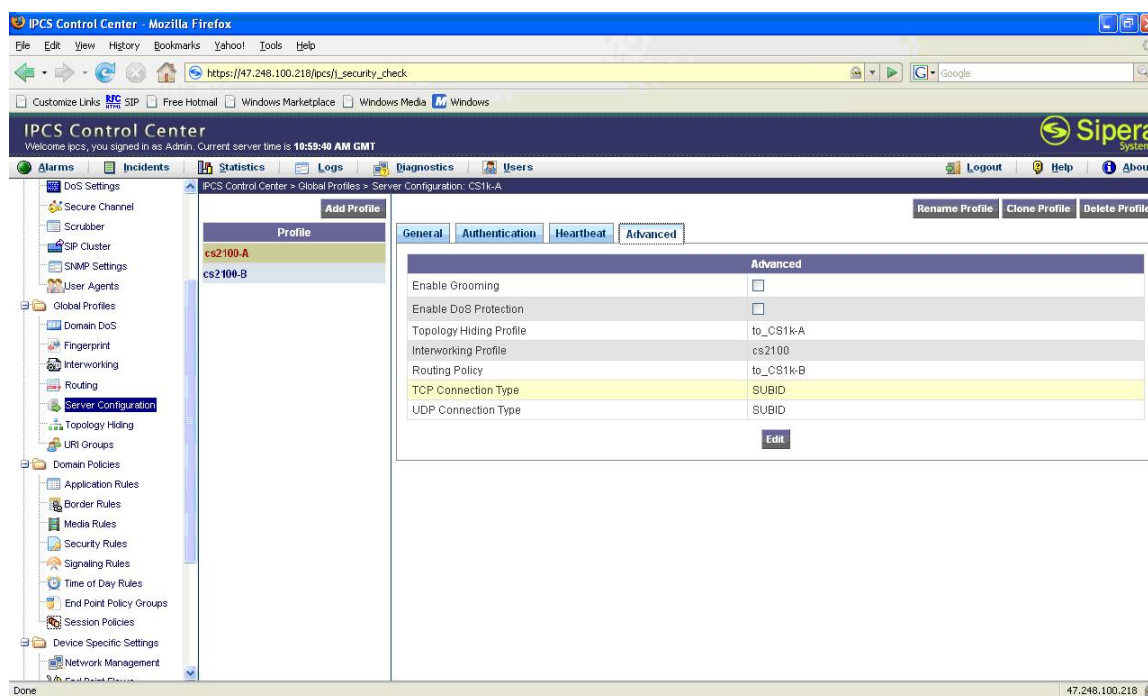
A server configuration must be established for both the line-side and trunk-side CS 2100 servers. The ‘Server Configuration’ is a set of properties along with a list of actions that UC-Sec will perform when SIP packets are received from the CS 2100 server defined in this ‘Server Configuration’. The following diagram shows the ‘General’ configuration tab including the defined supported transports and port numbers to be used when communicating with the line-side CS 2100 server.



Step 11: Server Configuration for Line-side CS 2100 – Advanced

Goto “Global Profiles” → “Server Configuration” → “Add Profile”

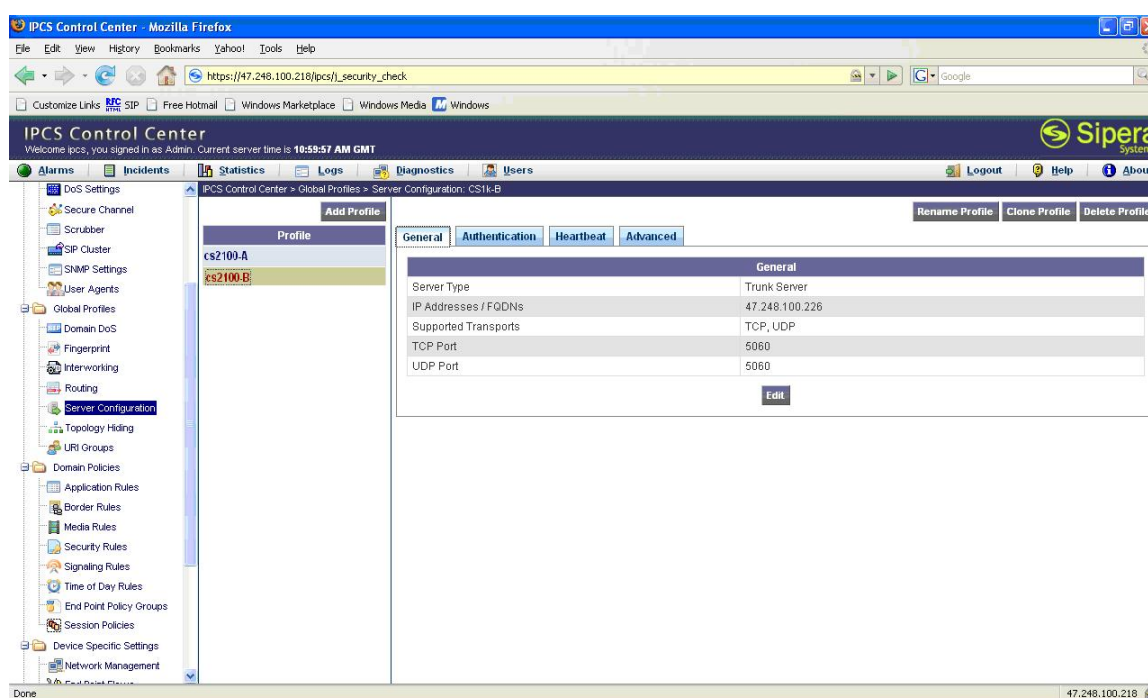
A server configuration must be established for both the line-side and trunk-side CS 2100 servers. The ‘Server Configuration’ is a set of properties along with a list of actions that UC-Sec will perform when SIP packets are received from the CS 2100 server defined in this ‘Server Configuration’. The following diagram shows the ‘Advanced’ configuration tab including the ‘Topology Hiding’ profile, ‘Routing policy’ and ‘Interworking Profile’, for this ‘Server Configuration’.



Step 12: Server Configuration for Trunk-side CS 2100 - General

Goto “Global Profiles” → “Server Configuration” → “Add Profile”

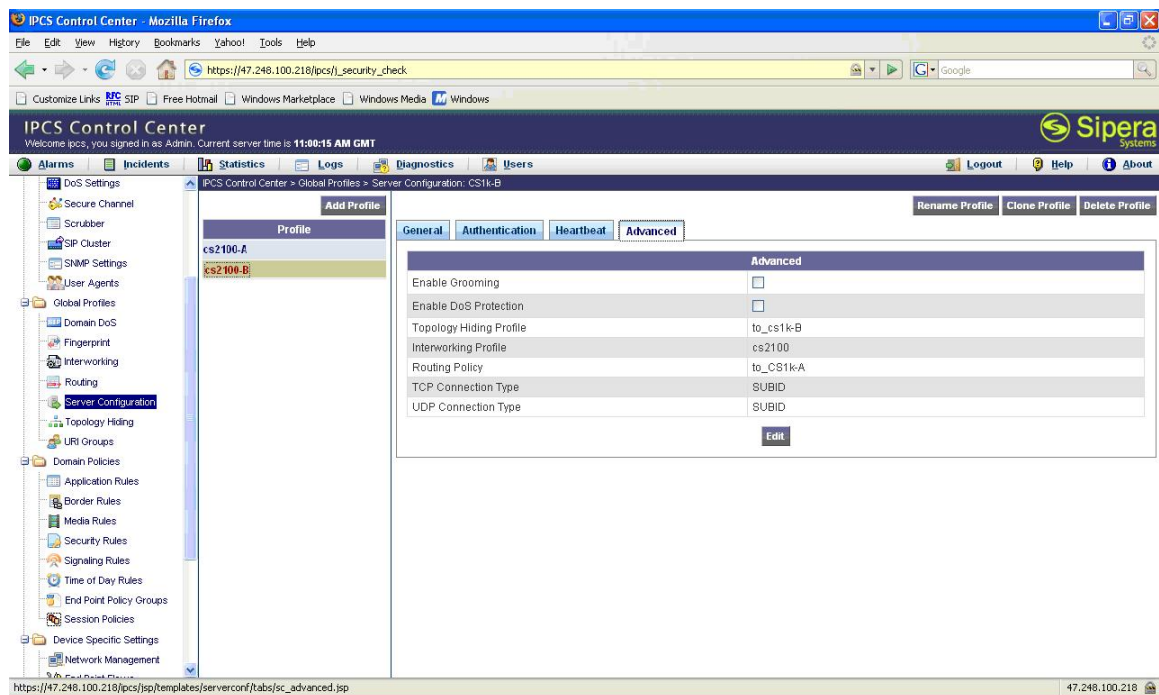
A server configuration must be established for both the line-side and trunk-side CS 2100 servers. The ‘Server Configuration’ is a set of properties along with a list of actions that UC-Sec will perform when SIP packets are received from the CS 2100 server defined in this ‘Server Configuration’. The following diagram shows the ‘General’ configuration tab including the supported transports and the port numbers which will be used when communicating with the trunk-side CS 2100 server.



Step 13: Server Configuration for Trunk-side CS 2100 - Advanced

Goto “Global Profiles” → “Server Configuration” → “Add Profile”

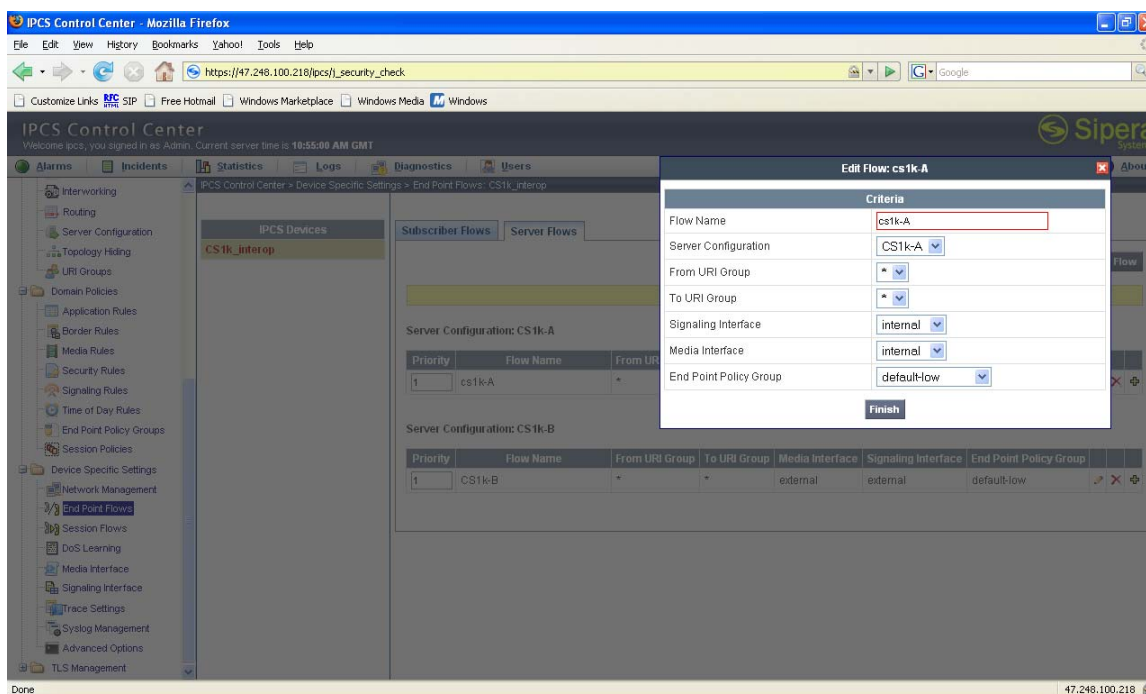
A server configuration must be established for both the line-side and trunk-side CS 2100 servers. The ‘Server Configuration’ is a set of properties along with a list of actions that UC-Sec will perform when SIP packets are received from the CS 2100 server defined in this ‘Server Configuration’. The following diagram shows the ‘Advanced’ configuration tab, including the ‘Topology Hiding’ profile, ‘Routing Policy’ and ‘Interworking Profile’ for this ‘Server Configuration’.



Step 14: Server Flows for Line-side CS 2100

Goto “Device Specific Settings” → “Server Flows” → “Add Flow”

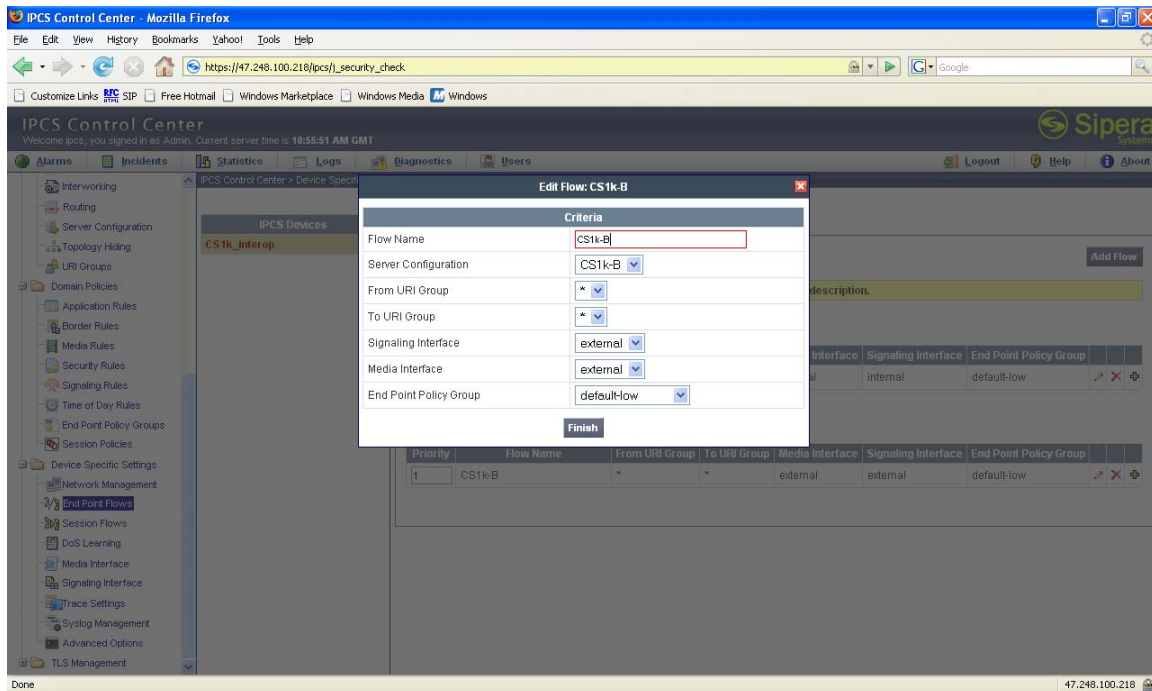
Server flows must be configured for both the line-side and trunk-side CS 2100 servers. The following configuration shows that any SIP and RTP packets arriving on the internal signaling and media interfaces are tied to the server flow for CS 2100-A, which is the line-side server. The properties defined in the ‘Server Configuration’ named ‘CS 2100-A’ and the ‘End-Point Policy Group’ named ‘default-low’ are applied to this server flow. The ‘End-Point Policy Group’ is a set of security configuration profiles for a particular group. As the security configuration is not within the scope of this document, a detailed configuration and explanation is not provided.



Step 15: Server Flows for Trunk-side CS 2100

Goto “Device Specific Settings” → “Server Flows” → “Add Flow”

Server flows must be configured for both the line-side and trunk-side CS 2100 servers. The following configuration shows that any SIP and RTP packets arriving on the external signaling and media interfaces are tied to the server flow for CS 2100-B which is the trunk-side server. The properties defined in ‘Server Configuration’ named ‘CS 2100-B’ and the ‘End-Point Policy Group’ named ‘default-low’ are applied to this server flow. The ‘End-Point Policy Group’ is a set of security configuration profiles for a particular group. As the security configuration is not within the scope of this document, a detailed configuration and explanation is not provided.

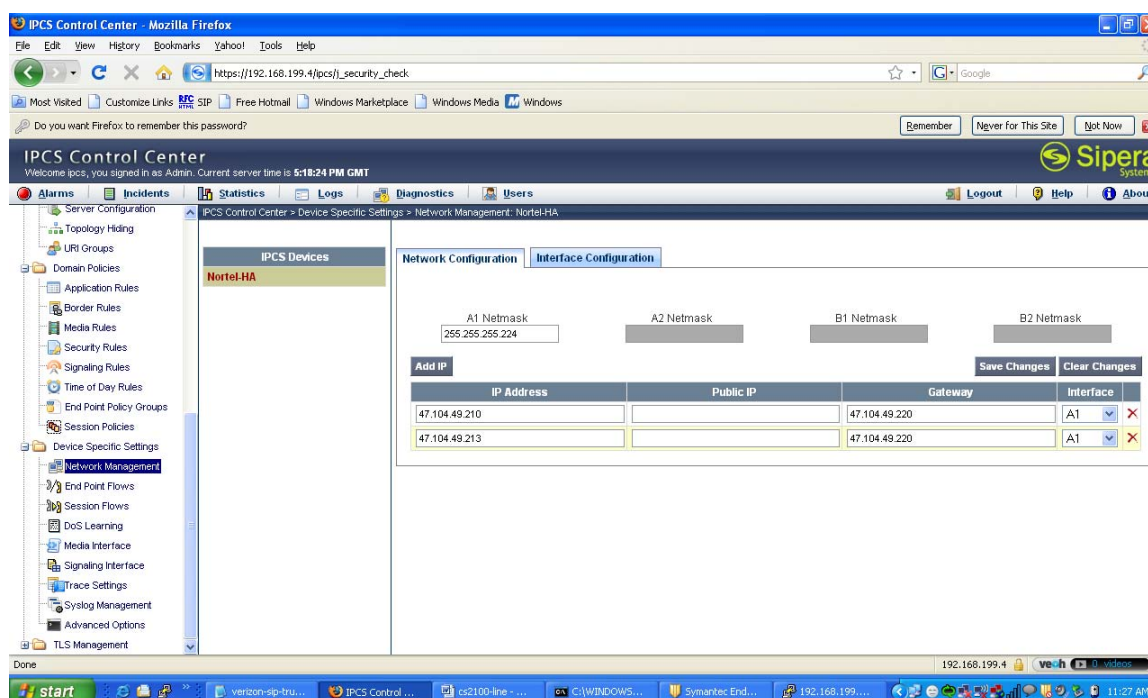


Configuration Steps (SIP Line-Side)

Step 1: IP Addresses

Goto “Device Specific Settings” → “Network Management” → “Network Configuration”

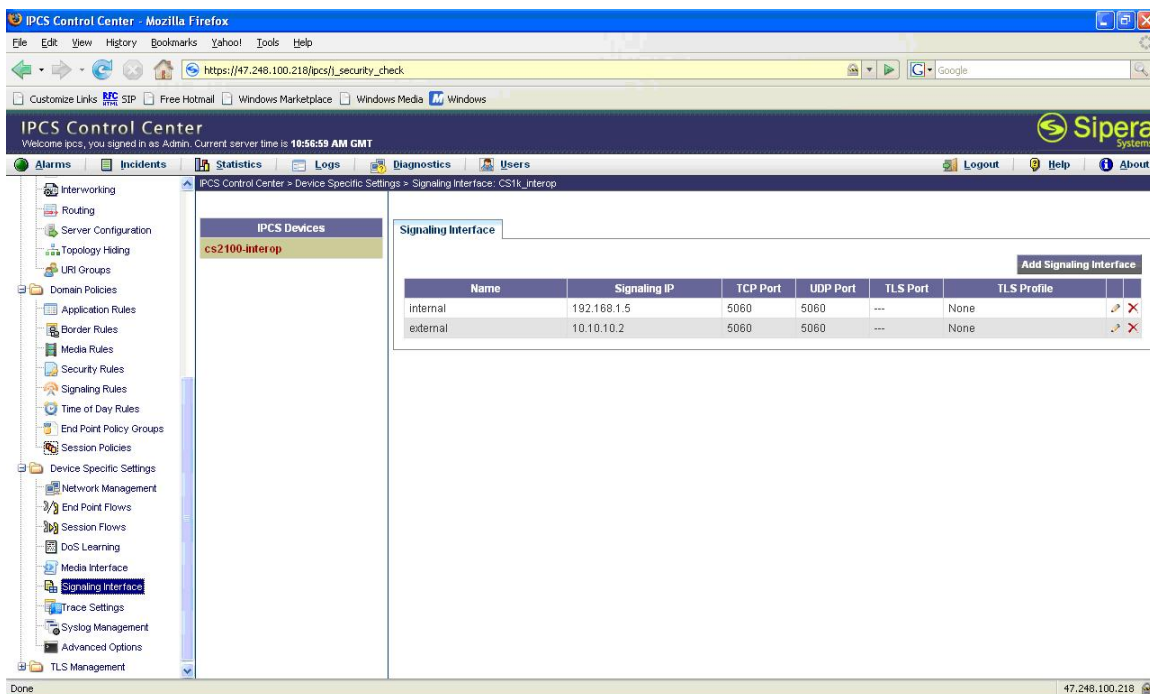
Configure the IP addresses, subnet mask and the default gateways for the network interfaces on UC-Sec. This step requires the configuration of a minimum of two IP addresses, one for communication between UC-Sec and CS 2100, and the other for communication between UC-Sec and phones. The two IP addresses, if on the same subnet, can be configured on the same network interface (single-wire mode). If the IP addresses are on different subnets, they must be configured on two separate network interfaces (two-wire mode).



Step 2: Signaling Interfaces

Goto “Device Specific Settings” → “Signalling Interface” → “Add Signaling Interface”

The signaling interfaces for the IP addresses already configured on the UC-Sec must be configured with the transport protocol supported on each interface. This will be used for signaling to a logical name, which will later be tied to Server flows and Subscriber flows.



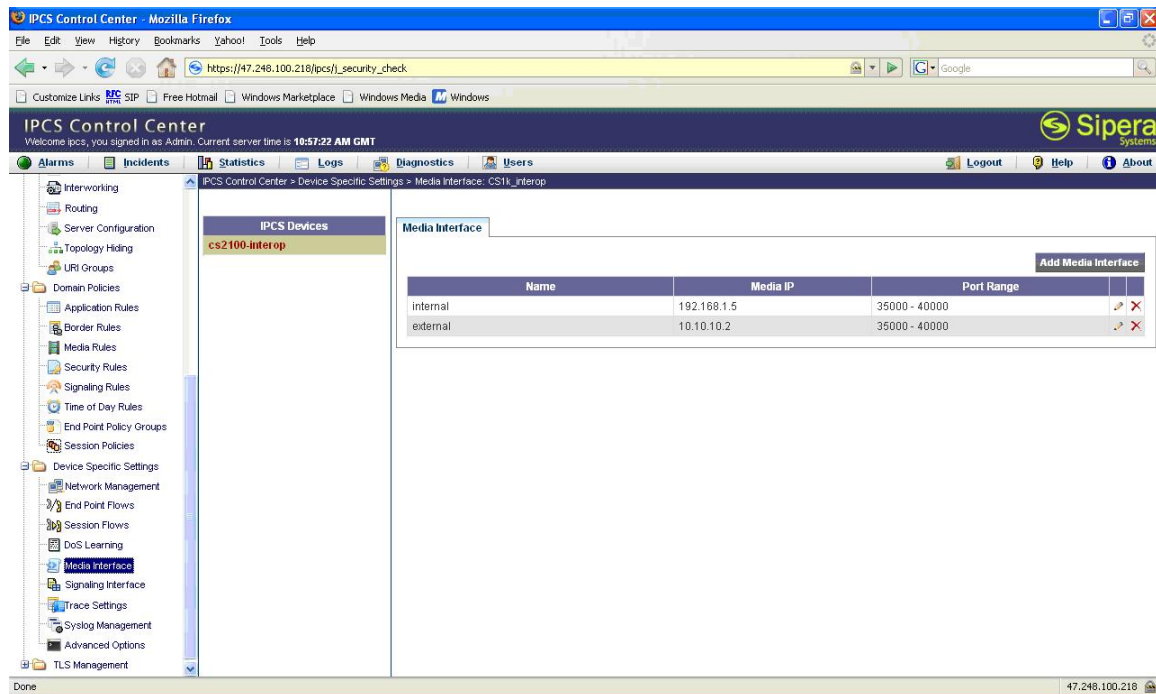
The screenshot shows the IPCS Control Center web interface in a Mozilla Firefox browser. The address bar shows the URL https://47.248.100.218/ipcs/_security_check. The interface includes a navigation menu on the left with categories like Interworking, Routing, Server Configuration, and Device Specific Settings. The 'Signaling Interface' option under 'Device Specific Settings' is selected. The main content area displays the 'Signaling Interface' configuration for the device 'cs2100-interop'. It includes a table with columns for Name, Signaling IP, TCP Port, UDP Port, TLS Port, and TLS Profile. There are two entries: 'internal' and 'external'. An 'Add Signaling Interface' button is located at the top right of the table.

Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile
internal	192.168.1.5	5060	5060	---	None
external	10.10.10.2	5060	5060	---	None

Step 3: Media Interfaces

Goto “Device Specific Settings” → “Media Interface” → “Add Media Interface”

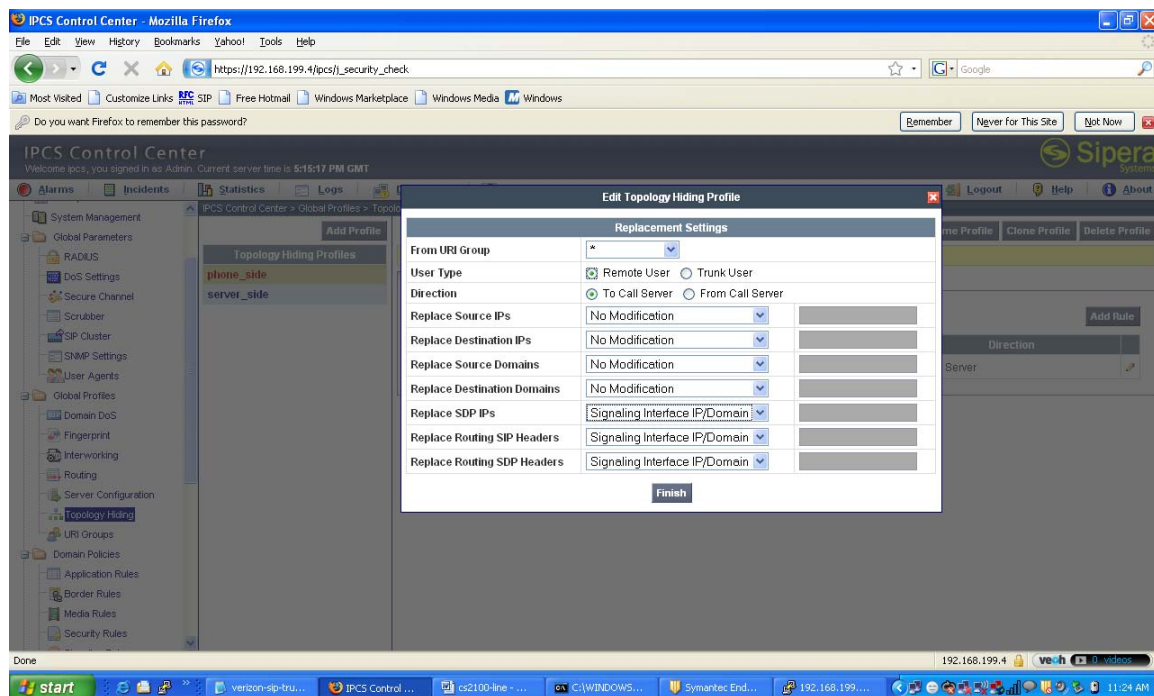
The media interfaces for the IP addresses already configured on the UC-Sec must be configured to assign a logical name to the port ranges used for RTP. This will be tied to Server flows and subscriber flows.



Step 4: Topology Hiding Profile (Phone side)

Goto “Global profiles” → “Topology hiding” → “Add profile”

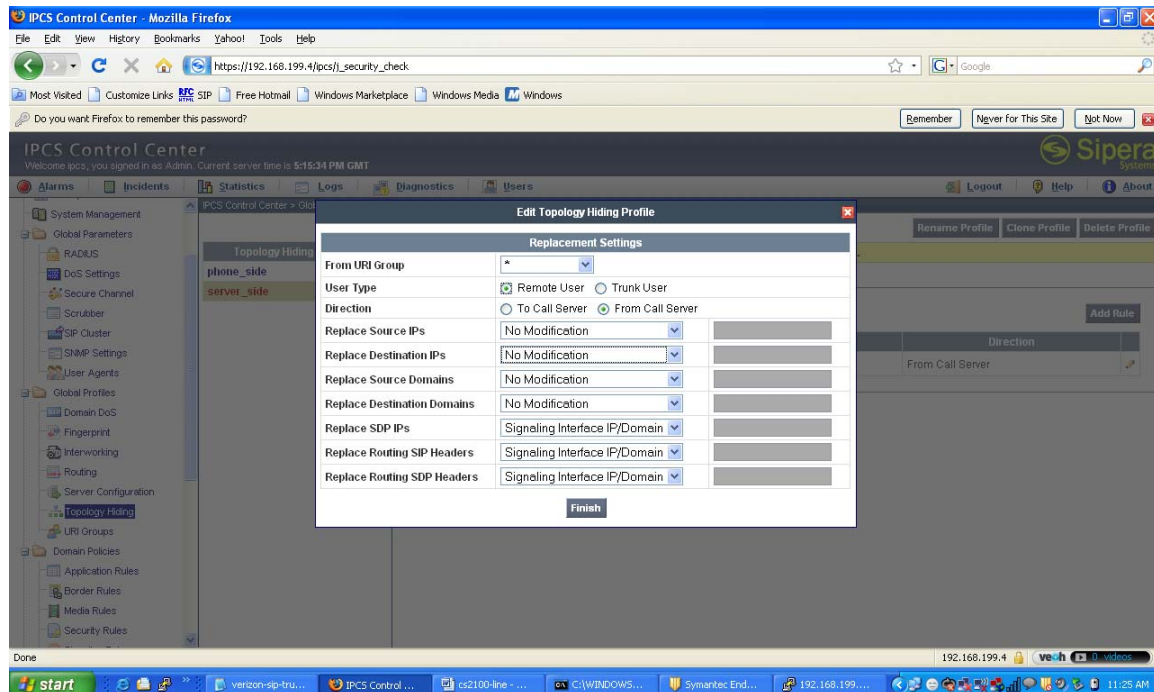
Topology hiding enables hiding the topology of the internal network from external and vice-versa (This is accomplished by stripping the routing entries and preserving what is needed). The flexibility to make changes to the routing headers and request URI is also offered. The default topology hiding profile for a ‘remote user’ case on the phone side is shown below.



Step 5: Topology Hiding Profile (Server side)

Goto “Global profiles” → “Topology hiding” → “Add profile”

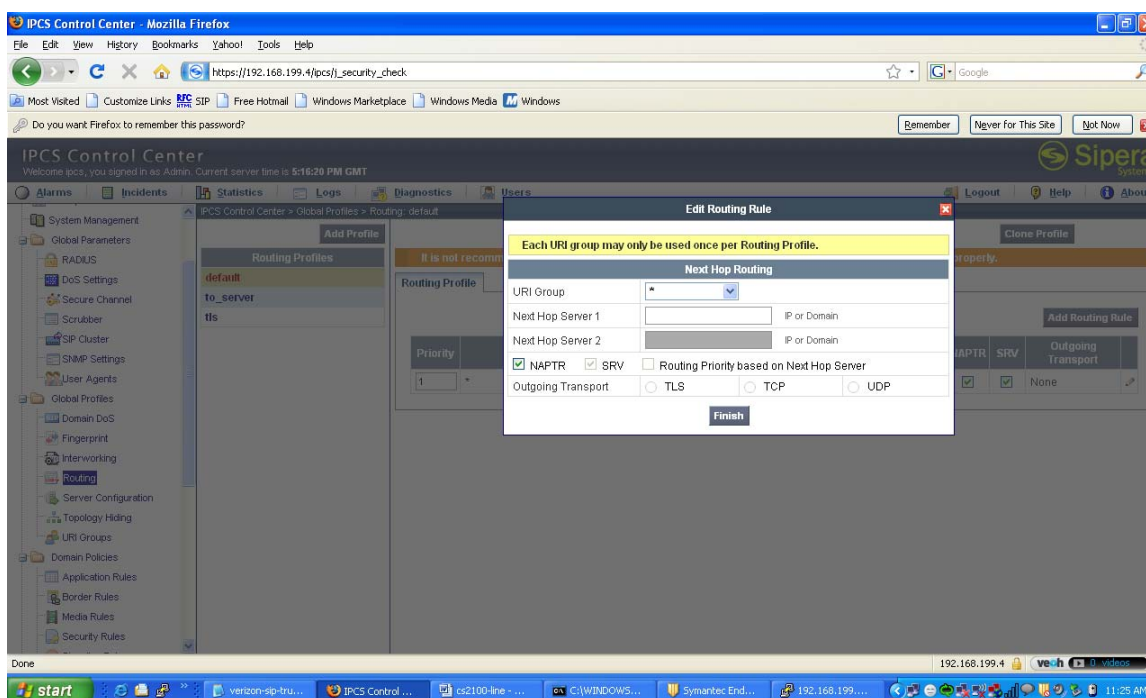
Topology hiding enables hiding the topology of internal network from external and vice-versa (This is accomplished by stripping the routing entries and preserving what is needed) . The flexibility to make changes to the routing headers and request URI is offered. The default topology hiding profile for a ‘remote user’ case on the server side is shown below.



Step 6: Routing Profile (Phone side)

Goto ‘Global Profiles’ → ‘Routing’ → ‘Add Profile’

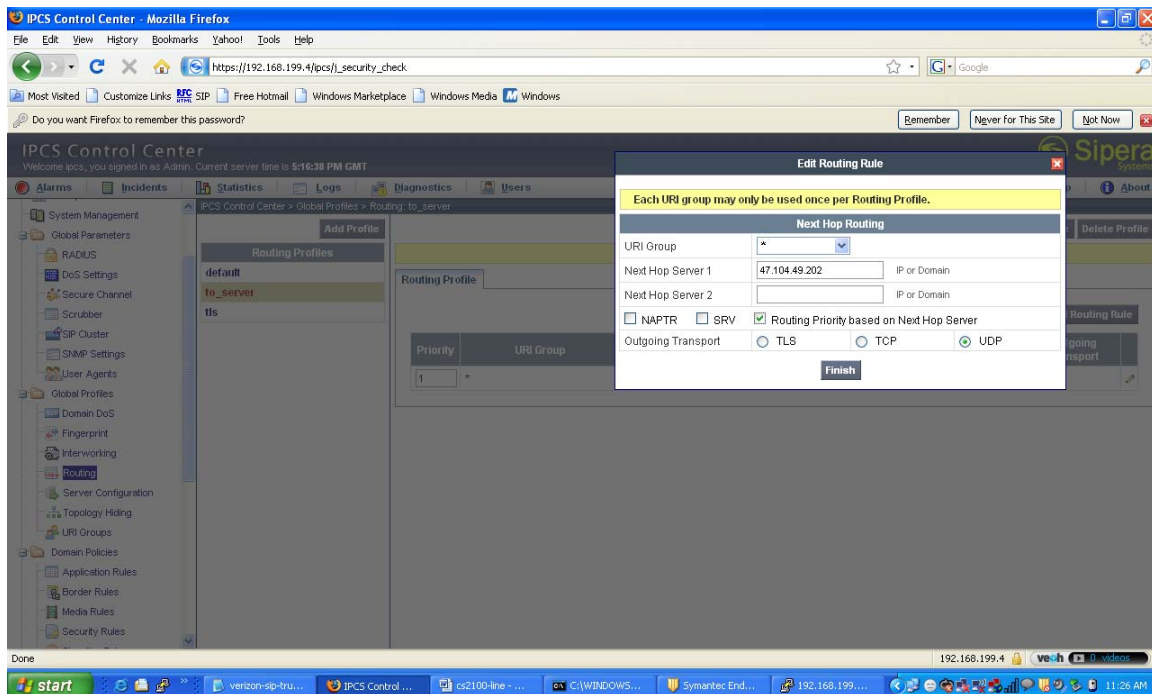
Routing profiles define where SIP packets will be routed when the profile is used in a ‘Server Configuration’ or ‘subscriber flow’. The routing can either be ‘Next Hop Server’-based or based on DNS (NAPTR, SRV) lookups. The configuration provided below is ‘Next Hop Server’-based. This profile is used in the subscriber flow so that, when a SIP request comes from a subscriber, a decision of which server the request should be routed to can be made.



Step 7: Routing Profile (Server side)

Goto 'Global Profiles' → 'Routing' → 'Add Profile'

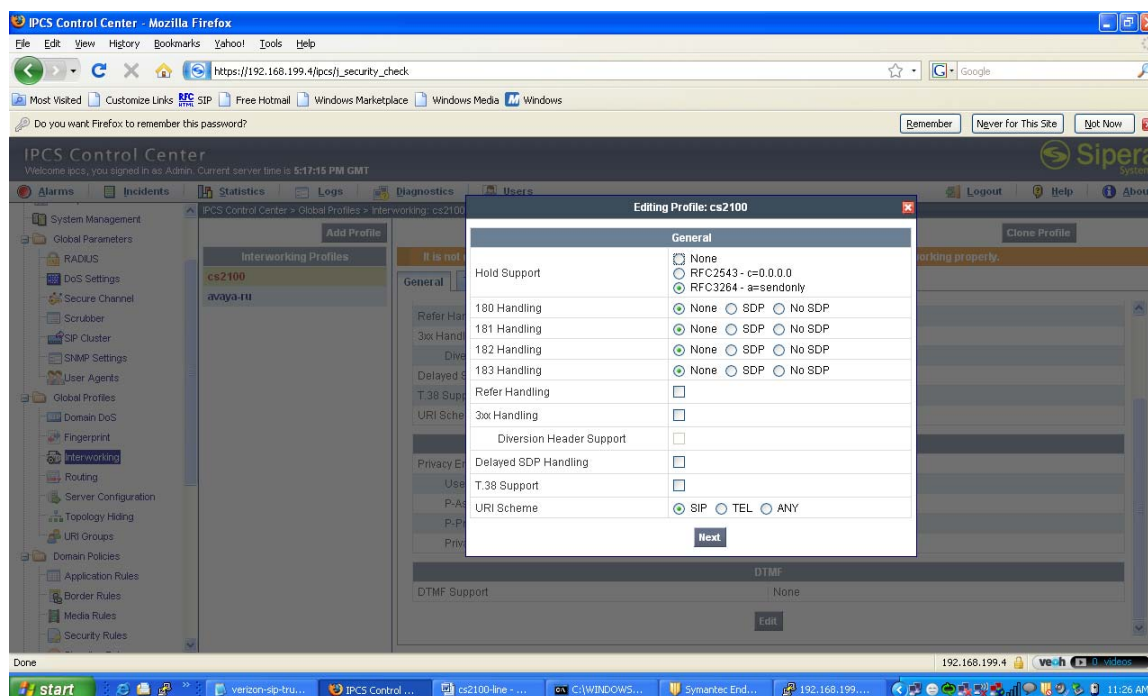
Routing profiles define where SIP packets will be routed when the profile is used either in the 'Server Configuration' or 'subscriber flow'. The routing can either be 'Next Hop Server'-based or based on DNS (NAPTR, SRV) lookups. The configuration provided below is DNS based. This profile is used in the server flow so that when a SIP request comes from the server, a decision on which subscriber the SIP requests should be sent to can be made.



Step 8: CS 2100 Interworking Profile – General Tab

Goto ‘Global Profiles’ → ‘Interworking’ → ‘Add Profile’

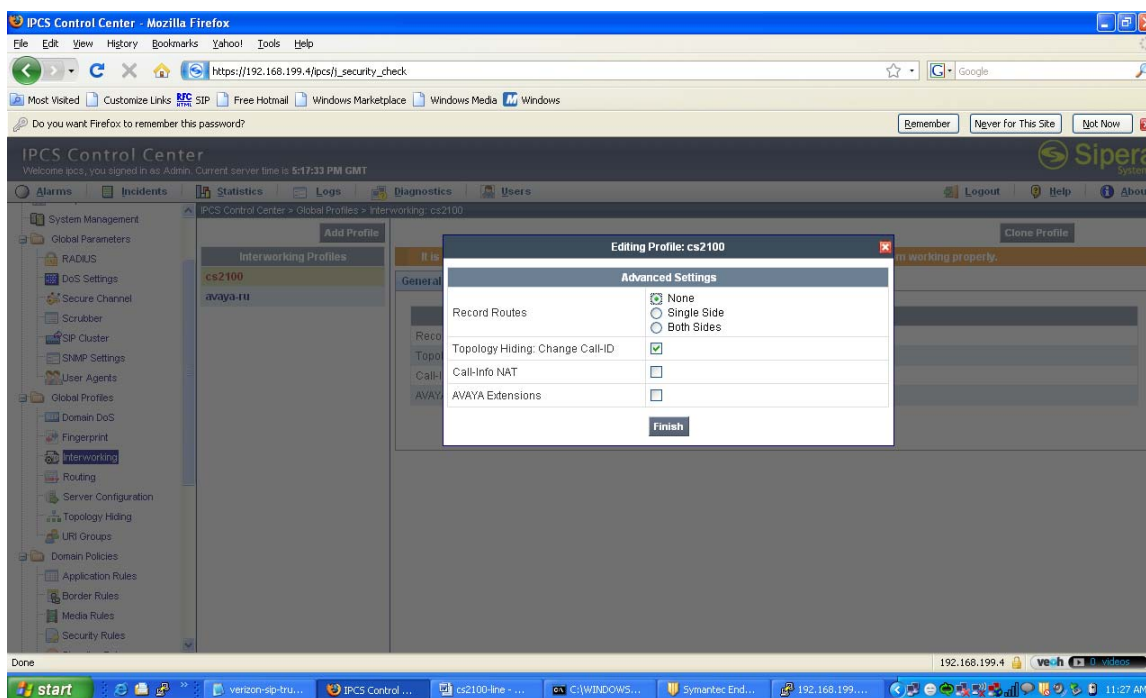
Interworking profiles improve interoperability by enabling communication between servers and phones from different vendors. An interworking profile for CS 2100 is provided below. This profile defines the message handling by UC-Sec for various messages when communicating to a CS 2100. The profile will be linked to the ‘Server Configuration’. The following screen shows the configuration under the ‘General’ tab in the ‘Interworking Profile’ for CS 2100.



Step 9: CS 2100 Interworking Profile – Advanced Tab

Goto ‘Global Profiles’ → ‘Interworking’ → ‘Add Profile’

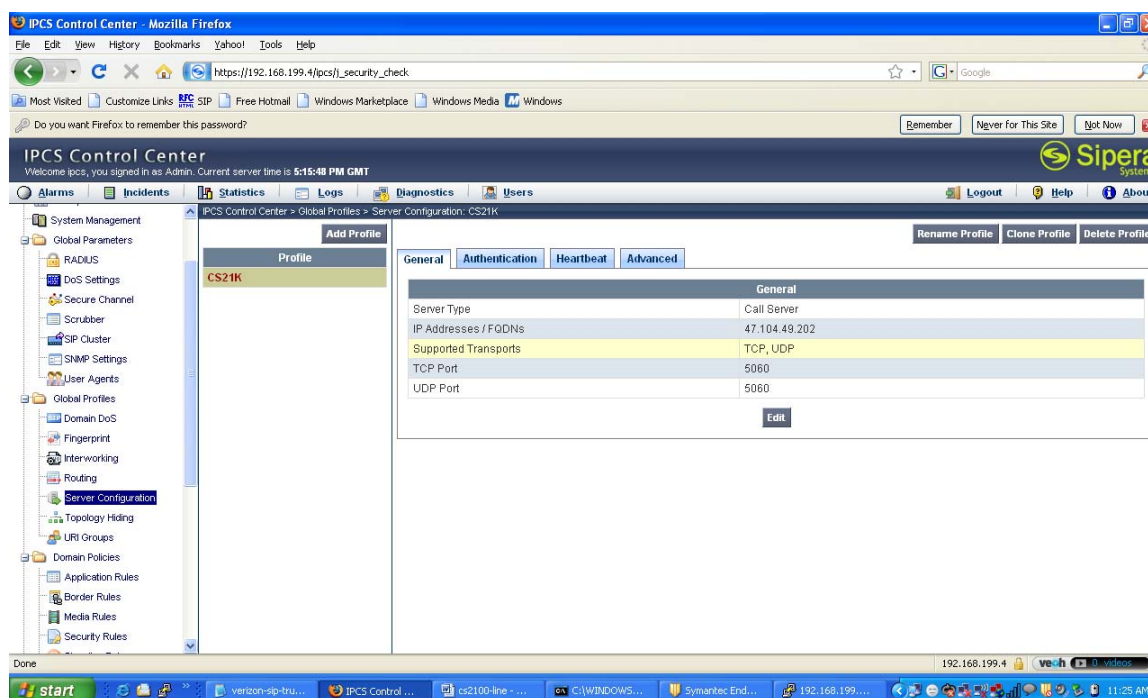
Interworking profiles improve interoperability by enabling communication between servers and phones from different vendors. An interworking profile for CS 2100 is provided below. This profile defines the message handling by UC-Sec for various messages when communicating to a CS 2100. This profile will be linked to the ‘Server Configuration’. The following screen shows the configuration under the ‘Advanced’ tab in the ‘Interworking Profile’ for CS 2100.



Step 10: Server configuration

Goto “Global Profiles” → “Server Configuration” → “Add Profile”

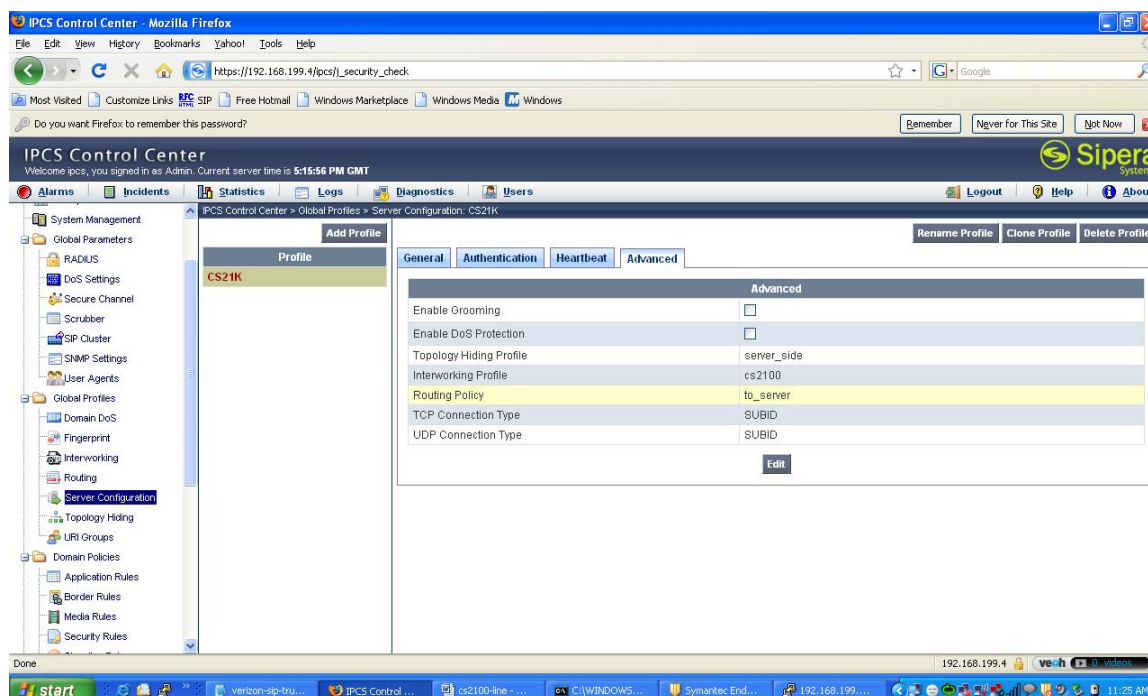
The ‘Server Configuration’ is a set of properties along with a list of actions that UC-Sec will perform when SIP packets are received from the CS 2100 server defined in this ‘Server Configuration’. The following diagram shows the ‘General’ configuration tab including the defined supported transports and port numbers to be used when communicating with the line-side CS 2100 server.



Step 11: Server Configuration for Line-side CS 2100 – Advanced

Goto “Global Profiles” → “Server Configuration” → “Add Profile”

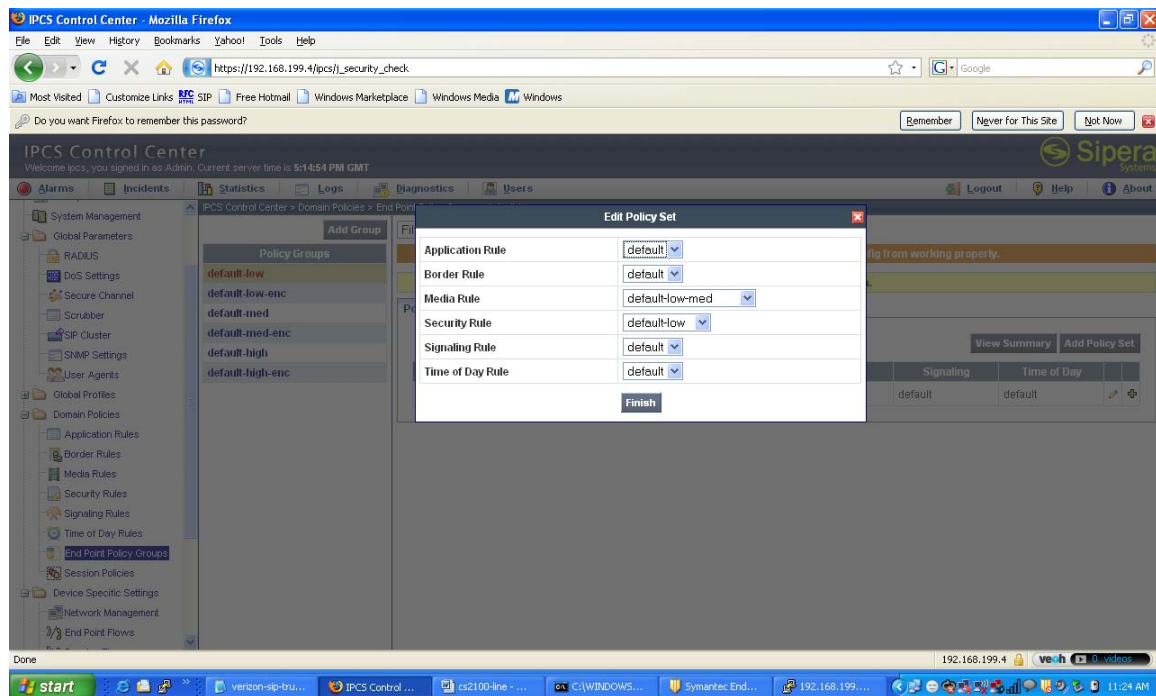
The ‘Server Configuration’ is a set of properties along with a list of actions that UC-Sec will perform when SIP packets are received from the CS 2100 server defined in this ‘Server Configuration’. The following diagram shows the ‘Advanced’ configuration tab including the ‘Topology Hiding’ profile, ‘Routing policy’ and ‘Interworking Profile’, for this ‘Server Configuration’.



Step 12: End Point Policy Group

Goto “Domain Policies” → “End Point Policy Groups” → “Add Group”

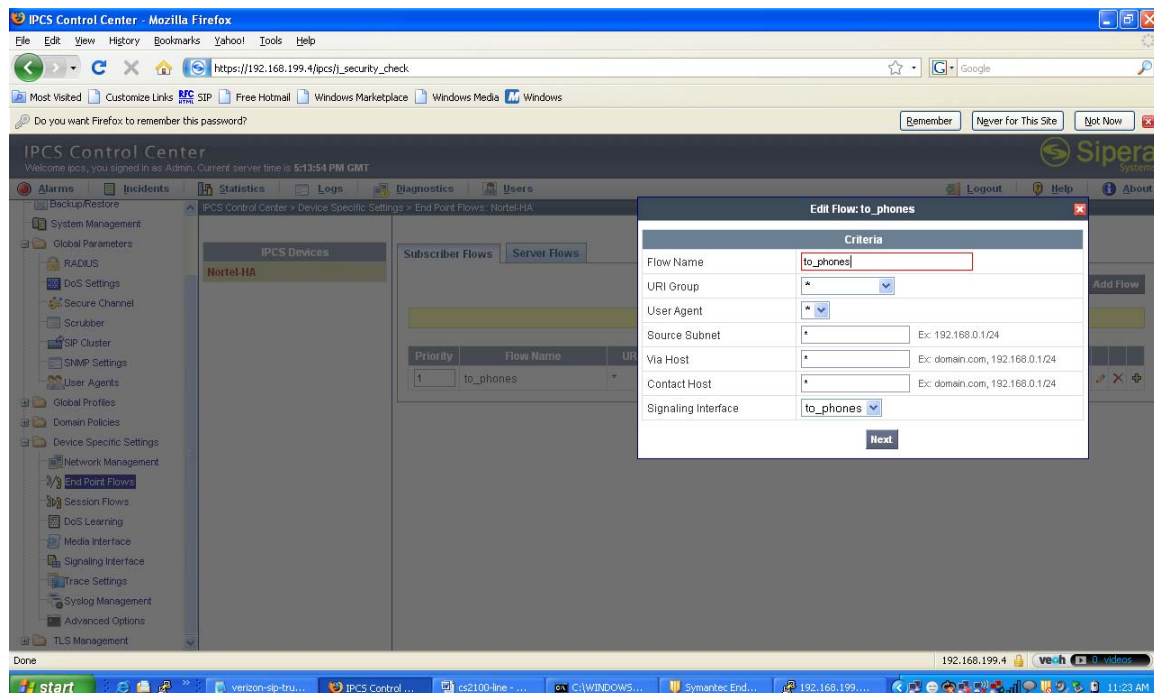
An End Point Policy Group is a set of security properties united as one group and which will be used later in “Subscriber flows” and “Server flows”. The security properties are divided into categories such as “Application rule”, “Border rule”, “Media rule”, “Security rule”, “Signaling rule” and “Time of day rule”.



Step 13: Subscriber Flows

Goto “Device Specific Settings” → “End Point Flows” → “Subscriber Flows”

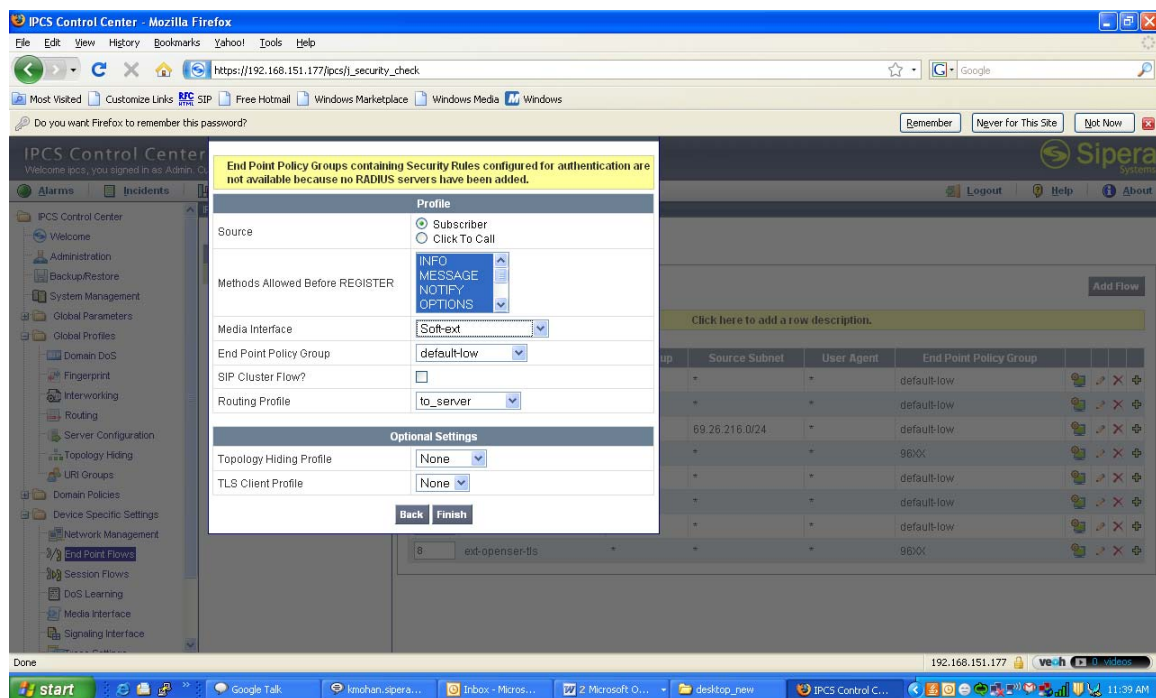
Subscriber flows are configured in order to identify the SIP signaling that comes from phones and to apply the appropriate rules to control various parameters. The following configuration shows that any SIP signaling arriving on the “to phones” signaling interface is tied to the subscriber flow named “to phones”.



Step 14: Subscriber Flows(cont'd)

Goto “Device Specific Settings” → “End Point Flows” → “Subscriber Flows”

The following screen, which is a continuation of the subscriber flow configuration, shows the parameters which can be controlled once the SIP signaling is identified as being that of a subscriber.



Step 15: Server Flows

Goto “Device Specific Settings” → “Server Flows” → “Add Flow”

Server flows must be configured in order to identify the SIP signaling that is sourced from the server and to apply certain properties once the SIP messages are identified as coming from server. The following configuration shows that any SIP and RTP packets arriving on the signaling and media interfaces named “to_CS21K” are tied to the server flow named “to_CS21k”. The properties defined in ‘Server Configuration’ named ‘CS 21K’ and the ‘End-Point Policy Group’ named ‘default-low’ are applied to this server flow. The ‘End-Point Policy Group’ is a set of security configuration profiles for a particular group.

