Avaya Solution & Interoperability Test Lab

Application Notes for Configuring the Sipera Systems IPCS 310 in an Avaya SIP Telephony Environment – Issue 1.0

Abstract

These Application Notes describe the configuration of the Sipera Systems IPCS 310 Security Appliance in an Avaya SIP Telephony environment consisting of Avaya SIP Enablement Services, Avaya Communication Manager, Avaya 4600 Series SIP and IP Telephones, and Avaya SIP and IP Softphones. The IPCS 310 is an IP communications security appliance that protects real-time multimedia applications (voice, video, IM), end-users, and the network infrastructure from VoIP attacks (DoS, Flood, SPAM) and misuse. Information in these Application Notes has been obtained through compliance testing and technical discussions. Testing was conducted via the Developer*Connection* Program at the Avaya Solution and Interoperability Test Lab in Lincroft, NJ.

1. Introduction

These Application Notes describe the configuration of the Sipera Systems IPCS 310 in an Avaya SIP Telephony environment consisting of Avaya SIP Enablement Services, Avaya Communication Manager, Avaya 4600 Series SIP and IP Telephones, and Avaya SIP and IP Softphones.

The IPCS 310 is a security appliance that protects signaling traffic for VoIP calls from malicious real-time attack. It incorporates a complete suite of VoIP-specific security techniques, including VoIP protocol anomaly detection and filtering, behavioral learning-based anomaly detection, and “gray area” analysis, verification and filtering. Together, these techniques monitor, detect, and protect VoIP networks from security vulnerabilities. The IPCS approach also has the advantage of centralizing the VoIP security administration and control currently implemented in many separate security devices (e.g., application-aware firewall, Intrusion Detection System (IDS), Intrusion Prevention System (IPS), DoS attack protection system).

As shown in **Figure 1**, the IPCS 310 is configured to protect the Avaya servers from attack. The servers include a multi-home Avaya SIP Enablement Services configuration with SIP trunks to Avaya Communication Manager. The IPCS 310 is inserted in the path of all traffic between the Avaya servers and clients. A pair of Ethernet interfaces on the IPCS bridges the Avaya C363T-PWR Converged Stackable Switch connecting the servers in the enterprise core to an identical model access switch connecting the clients. The IPCS 310 is configured to function transparently with respect to the enterprise network, requiring no special administration of the Avaya servers or clients. In transparent mode, the source and destination of SIP signaling messages is monitored actively and inspected for malicious VoIP traffic. Inspection of RTP media and TLS signaling traffic is planned for a future release.

The administration of the Avaya SIP infrastructure shown in **Figure 1** is not the focus of these Application Notes and will not be described. For administration of the network infrastructure shown in **Figure 1,** refer to the appropriate documentation listed in Section 8.

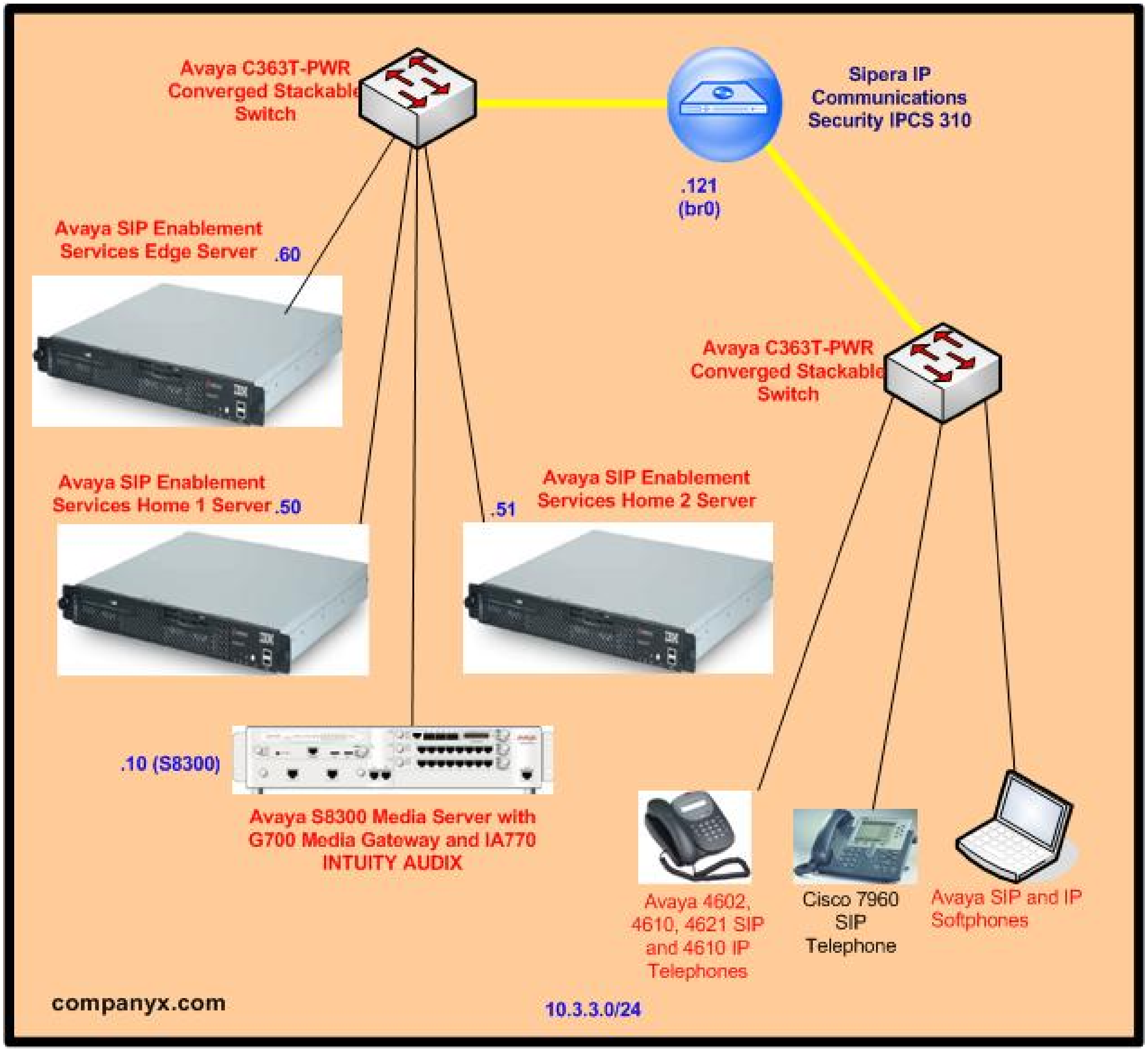

Avaya C363T-PWR Converged Stackable Switch
Sipera IP Communications Security IPCS 310
.121 (br0)
Avaya SIP Enablement Services Edge Server .60
Avaya C363T-PWR Converged Stackable Switch
Avaya SIP Enablement Services Home 1 Server .50
.51 Avaya SIP Enablement Services Home 2 Server
.10 (S8300)
Avaya S8300 Media Server with G700 Media Gateway and IA770 INTUITY AUDIX
Avaya 4602, 4610, 4621 SIP and 4610 IP Telephones
Cisco 7960 SIP Telephone
Avaya SIP and IP Softphones
companyx.com
10.3.3.0/24

Figure 1 – Network Configuration Diagram

2. Equipment and Software Validated

The following products and software were used for the configuration in **Figure 1**:

Equipment	Version
Avaya S8300 Media Server with G700 Media Gateway and IA770 INTUITY™ AUDIX®	
ICC	3.1 (Load 628.5)
VoIP Engine	60
MGP	25.23.0
Stack	4.1.6
IA770	N3.1-26.0
Avaya SIP Enablement Services	3.1 (Load 18)
Avaya C363T-PWR Converged Stackable Switch	4.5.14
Avaya 4602, 4610, 4621 SIP telephones	2.2.2
Avaya SIP Softphone	2.1 (Load 43)
Avaya 4610 Series H.323 telephone	2.3
Avaya IP Softphone	5.2 SP 1
PC for softphones	Microsoft Windows XP 2002 SP1
Cisco 7960 SIP Telephone	POS3-07-9-4
Sipera Systems IPCS 310	2.1.0.Q06.P02
Mozilla Firefox web browser	1.5.0.1

Table 1 – Equipment and Version

3. Configure the Sipera Systems IPCS 310

3.1. Front Panel Layout

The IPCS 310 front panel is shown in **Figure 2** below. From left to right, it consists of a status display, USB ports, console serial port, and six Ethernet ports. For administration purposes, the Ethernet ports are numbered *eth0* through *eth5*, from right to left, as shown. The Ethernet ports are also referred to using the labels shown on the front panel. Ports M1 and M2 are used for management access. Ports A1/A2 and B1/B2 are grouped as pairs of 10/100/1000 Mbps Ethernet interfaces used for VoIP network access, and are identified as bridges *br1* and *br0*, respectively. One port in a pair is connected to the protected "server" side, and the other to the unprotected "network" side. Each pair can be put into "port bypass" mode, during which all traffic between the server and network ports is transmitted without inspection. This mode is automatically activated during a power or IPCS application failure.

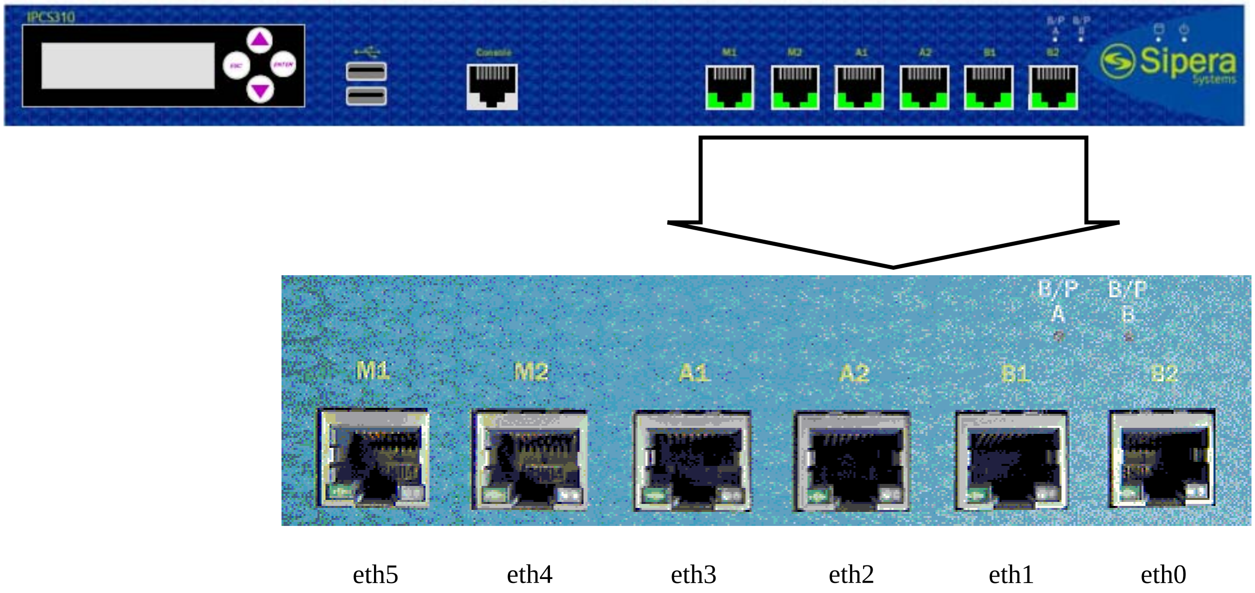


Figure 2 – IPCS 310 Front Panel

3.2. Installation

This section contains the command line interface steps for the installation of the IPCS 310. The IPCS 310 is installed using a PC connected to its console serial port, with the following settings.

Parameter	Value
Speed	19200
Data bits	8
Parity	None
Stop bits	1
Flow control	Hardware
Emulation	VT100

Table 2 – Serial Console Port Settings

When the system first boots up, it prompts for the machine name and the DNS domain name. No DNS is used in this configuration, so the default (blank) is used.

```
> IPCS Machine Name : avaya_ipcs
> IPCS Domain Name :
> Machine FQDN : avaya_ipcs
```

The IPCS 310 can also be accessed via one of the management Ethernet interfaces using the `ssh` service on port 222. In the example below, the M2 Ethernet port was used for this purpose. It is recommended that the management and signaling networks be separate, although this was not necessary for the sample configuration.

```
060221:091126:  ****************Management Configuration
****************
> Management Ethernet Interface Name : eth4
> Management Ethernet Interface IP  : 10.3.3.120
> Management Ethernet Interface Netmask : 255.255.255.0
> Management Gateway Address : 10.3.3.1
```

In the following command line sequence, the B1/B2 pair (bridge **br0**) is used for protecting the Avaya servers from attack. The "Server side" is the protected side (B1/**eth1**), and the "Network side" is treated as unprotected (B2/**eth0**). The bridge IP address (**10.3.3.121)** is used for verifying that the networks are reachable on both sides (see Section 5, Step 4). One of the servers to be protected is the SIP Enablement Services Edge server with IP address **10.3.3.60**. The remaining protected servers will be specified using the web-based administration interface (see Section 3.3).

```
060221:091129:  ****************First set of Bridge
Configuration ****************
> Bridge IP Address : 10.3.3.121
> Bridge Interface Name : br0
> Bridge Netmask : 255.255.255.0
> Network Side Ethernet Interface Slave Name : eth0
> Server Side Ethernet Interface Slave Name : eth1
> Gateway Address : 10.3.3.1
> Protected Server connected to this Bridge : 10.3.3.60
> Do you want to configure a second set of Bridge?[N]
```

Press the **Enter** key at the end of the above sequence to exit the installation script. Enter "Y" and the **Enter** key to configure the second pair of interfaces if required. After completing this install script, the Linux system will prompt for a login and password, which would permit use of the IPCS CLI (see Section 5).

Check the status display panel to verify that the IPCS application is running with no errors or warnings, as shown in **Figure 3** below. The first line of the display has the format <Threat Level>/<Hardware Status>/<Software Status>/<Port bypass mode>. The display in **Figure 3** indicates no threat, no hardware malfunction, no software error, and automatic port bypass mode is enabled.

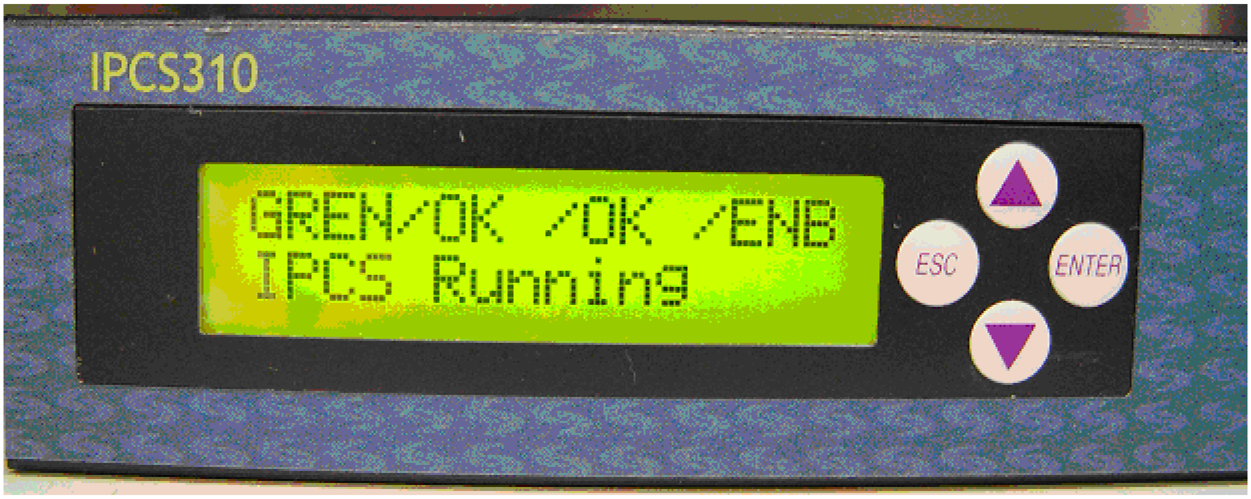
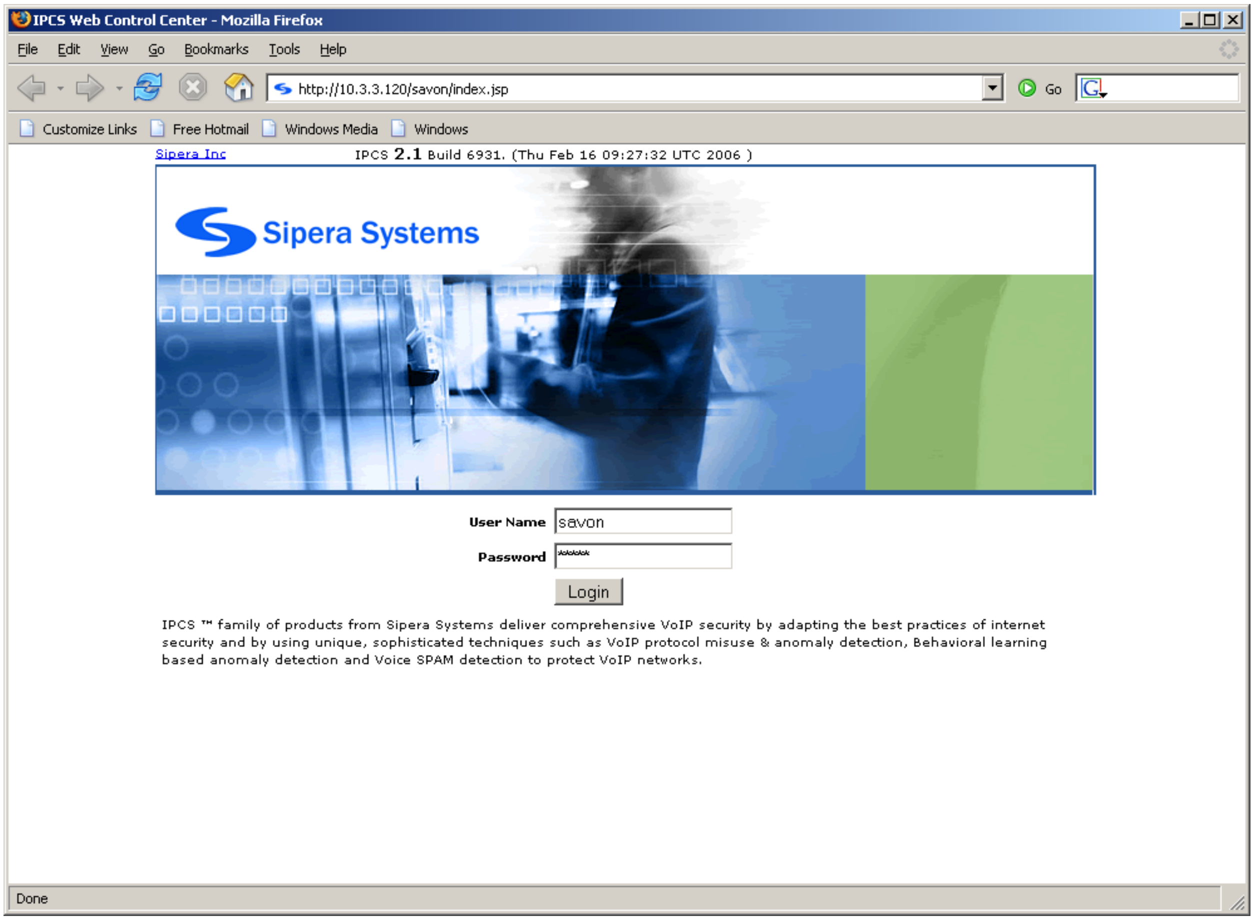


Figure 3 – Front Status Panel

3.3. Configuring additional protected servers

The command line installation steps in Section 3.2 included configuring protection for the first Avaya server (SIP Enablement Services Edge server in the sample configuration). This section describes the configuration of the IPCS 310 to protect additional servers. In the sample configuration, this includes the SIP Enablement Services Home 1 and Home 2 servers as well as the Avaya S8300 Media Server. The steps required to specify the servers to be protected are shown here. For additional details on configuring parameters related to the security features of the IPCS 310, refer to [6].

Steps	Description
1.	Access the web administration interface via the management Ethernet interface, using the Mozilla Firefox web browser, and log in. 

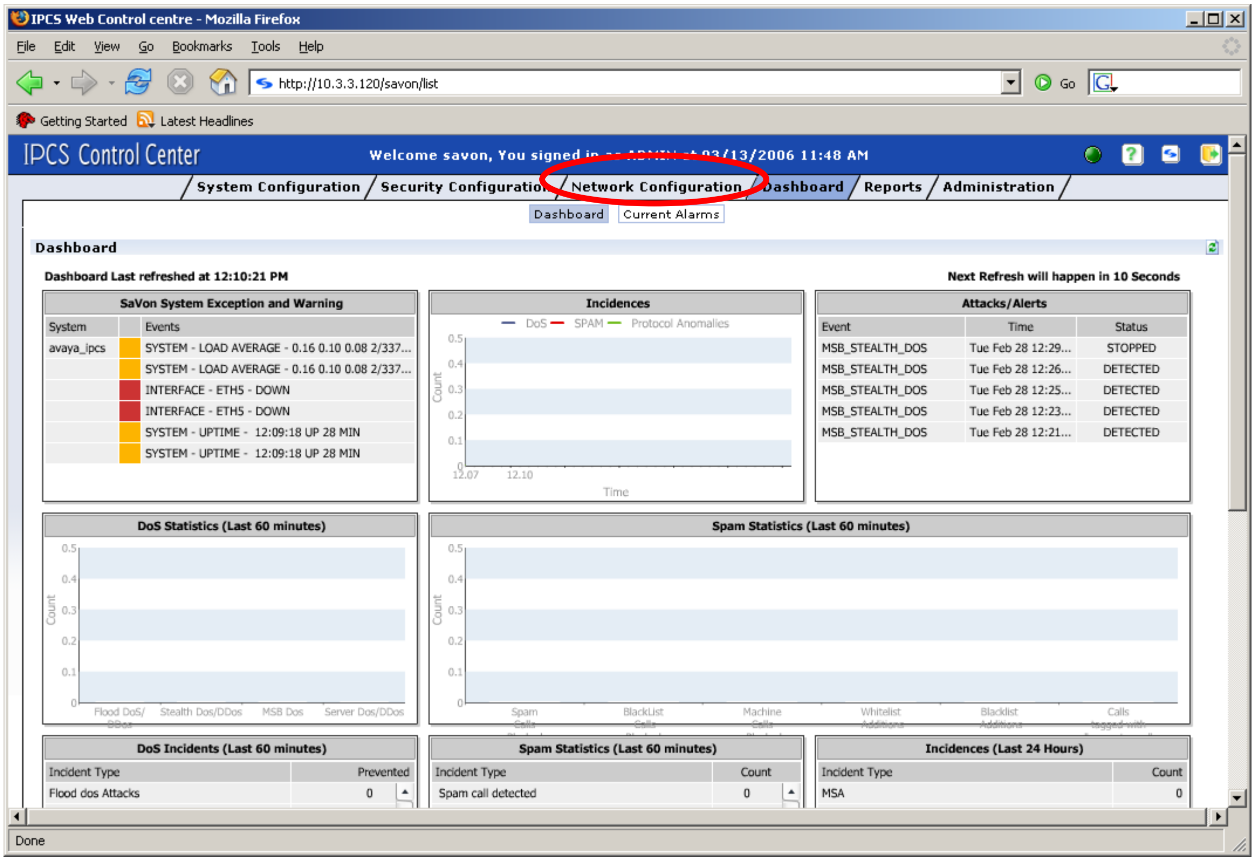
http://10.3.3.120/savon/index.jsp

IPCS 2.1 Build 6931. (Thu Feb 16 09:27:32 UTC 2006)

User Name savon

Password *****

IPCS ™ family of products from Sipera Systems deliver comprehensive VoIP security by adapting the best practices of internet security and by using unique, sophisticated techniques such as VoIP protocol misuse & anomaly detection, Behavioral learning based anomaly detection and Voice SPAM detection to protect VoIP networks.

Steps	Description
2.	The system dashboard will be displayed. Protect additional Avaya servers by clicking on the **Network Configuration** link. 

Welcome savon, You signed in as ADMIN at 03/13/2006 11:48 AM

Dashboard

Dashboard Last refreshed at 12:10:21 PM

Next Refresh will happen in 10 Seconds

SaVon System Exception and Warning

System		Events
avaya_ipcs	🟧	SYSTEM - LOAD AVERAGE - 0.16 0.10 0.08 2/337...
	🟧	SYSTEM - LOAD AVERAGE - 0.16 0.10 0.08 2/337...
	🟥	INTERFACE - ETH5 - DOWN
	🟥	INTERFACE - ETH5 - DOWN
	🟧	SYSTEM - UPTIME - 12:09:18 UP 28 MIN
	🟧	SYSTEM - UPTIME - 12:09:18 UP 28 MIN

Incidences

Attacks/Alerts

Event	Time	Status
MSB_STEALTH_DOS	Tue Feb 28 12:29...	STOPPED
MSB_STEALTH_DOS	Tue Feb 28 12:26...	DETECTED
MSB_STEALTH_DOS	Tue Feb 28 12:25...	DETECTED
MSB_STEALTH_DOS	Tue Feb 28 12:23...	DETECTED
MSB_STEALTH_DOS	Tue Feb 28 12:21...	DETECTED

DoS Statistics (Last 60 minutes)

Spam Statistics (Last 60 minutes)

DoS Incidents (Last 60 minutes)

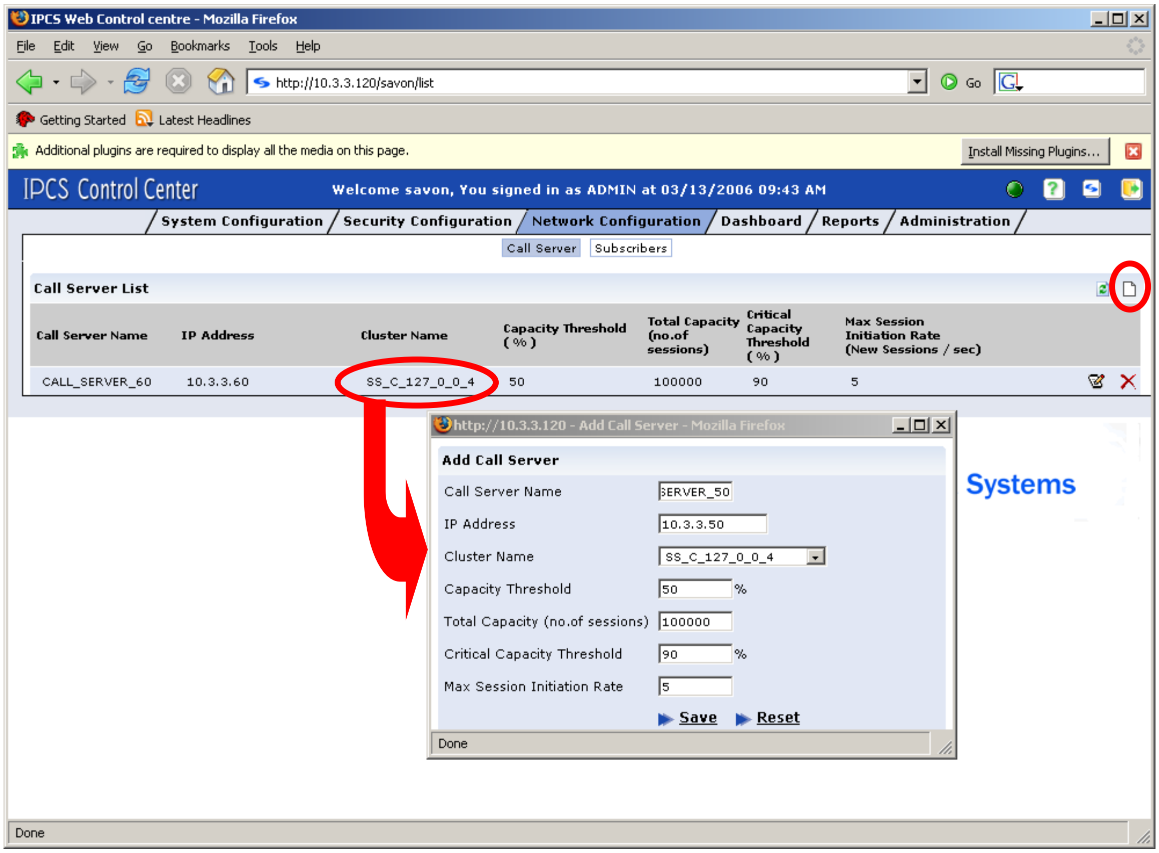
Incident Type	Prevented
Flood dos Attacks	0

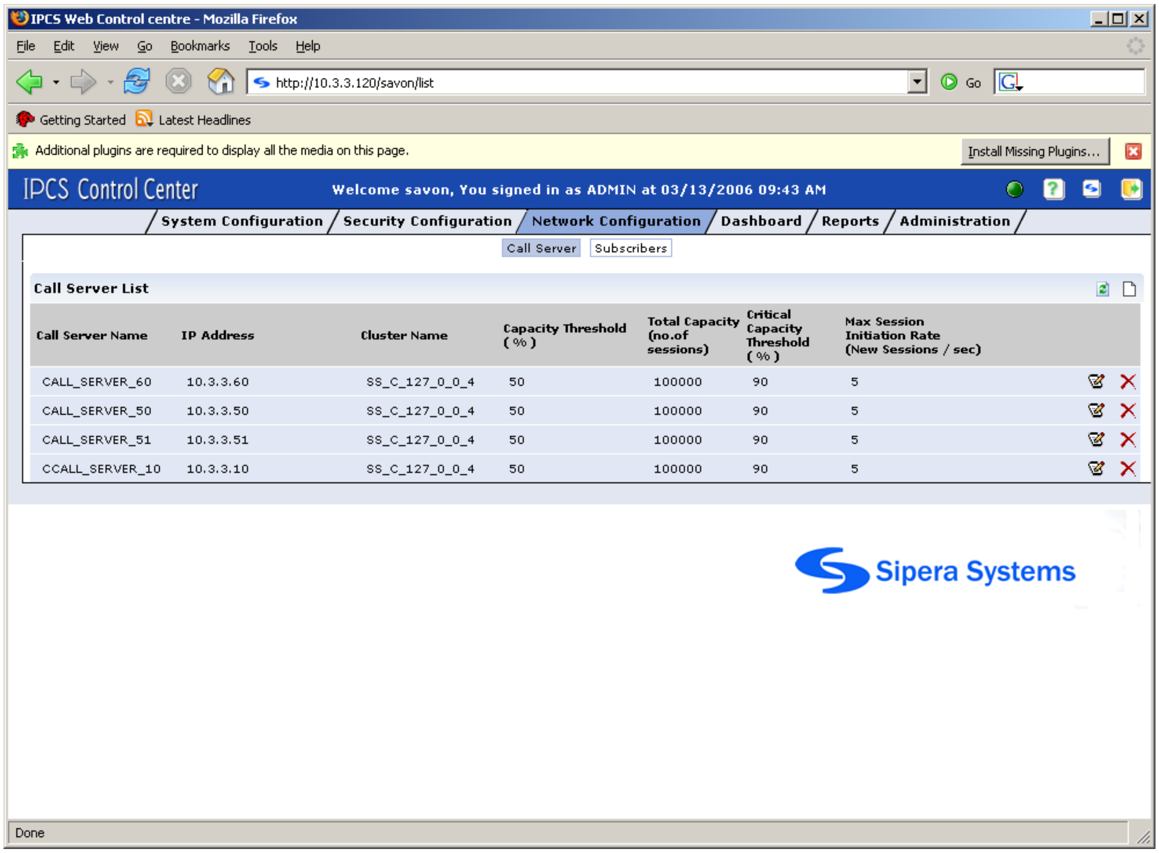
Spam Statistics (Last 60 minutes)

Incident Type	Count
Spam call detected	0

Incidences (Last 24 Hours)

Incident Type	Count
MSA	0

Steps	Description
3.	When the network configuration page is displayed, click on the icon circled in red to add another server. Fill in the dialog box that appears, including the **Call Server Name** and **IP Address** of the protected server. Use the pull-down menu to enter the same **Cluster Name** as the name automatically assigned to the first protected server entered during installation. The remaining parameters govern the protection thresholds, and are covered in [6]. The Avaya SIP Enablement Services Home 1 server was added in the example below. Click on **Save**.  IPCS Web Control centre - Mozilla Firefox http://10.3.3.120/savon/list Additional plugins are required to display all the media on this page. IPCS Control Center Welcome savon, You signed in as ADMIN at 03/13/2006 09:43 AM Call Server List Call Server Name: CALL_SERVER_60 · IP Address: 10.3.3.60 · Cluster Name: SS_C_127_0_0_4 · Capacity Threshold (%): 50 · Total Capacity (no.of sessions): 100000 · Critical Capacity Threshold (%): 90 · Max Session Initiation Rate (New Sessions / sec): 5 http://10.3.3.120 - Add Call Server - Mozilla Firefox Add Call Server Call Server Name: SERVER_50 IP Address: 10.3.3.50 Cluster Name: SS_C_127_0_0_4 Capacity Threshold: 50 % Total Capacity (no.of sessions): 100000 Critical Capacity Threshold: 90 % Max Session Initiation Rate: 5 ▶ Save ▶ Reset Done

Steps	Description
4.	Repeat Step 3 for each additional protected server. The following screen shows the resulting set of protected servers after the above step is performed for the Avaya SIP Enablement Services Home 1 and Home 2 servers and the Avaya S8300 Media Server. 

Additional plugins are required to display all the media on this page.

Welcome savon, You signed in as ADMIN at 03/13/2006 09:43 AM

Call Server List

Call Server Name	IP Address	Cluster Name	Capacity Threshold (%)	Total Capacity (no.of sessions)	Critical Capacity Threshold (%)	Max Session Initiation Rate (New Sessions / sec)
CALL_SERVER_60	10.3.3.60	SS_C_127_0_0_4	50	100000	90	5
CALL_SERVER_50	10.3.3.50	SS_C_127_0_0_4	50	100000	90	5
CALL_SERVER_51	10.3.3.51	SS_C_127_0_0_4	50	100000	90	5
CCALL_SERVER_10	10.3.3.10	SS_C_127_0_0_4	50	100000	90	5

4. Interoperability Compliance Testing

The Sipera Systems IPCS 310 was compliance tested to verify that it can interoperate with an Avaya IP Telephony environment. The IPCS currently supports inspection of SIP signaling traffic. It does not inspect media flows (RTP), or TLS and H.323 signaling traffic. Inspection of RTP and TLS traffic is planned for a future release.

4.1. General Test Approach

Based on the current capabilities of the IPCS 310, the tests were designed to verify that SIP signaling traffic, as implemented by Avaya server and client products, was not negatively affected by the insertion of the IPCS 310. Some testing of Avaya H.323 and TLS based signaling traffic was performed to verify that this traffic, although not inspected, was not blocked or altered.

The following scenarios were tested using the network configuration shown in **Figure 1**:

- Registration of all telephones and softphones
- Basic calling
- A subset of the SIPPING-19 [7] supplementary features (e.g., transfer, conference, call pickup, call answer back)
- Forwarding calls to the INTUITY™ AUDIX® voice messaging system, including use of DTMF to access menus.
- Mixed SIP and H.323 calls
- Presence and Instant Messaging features of Avaya SIP and IP Softphone.
- Enabling and disabling port bypass on the IPCS 310 by using the IPCS CLI (see Section 5, Step 5) as well as by powering cycling the IPCS

4.2. Test Results

All tests outlined above were completed successfully during the test period.

5. Verification Steps

The following verification steps can be used when troubleshooting configurations in the field. Since the IPCS 310 is intended to operate transparent to the rest of the network, the issues that can arise are mainly those of proper connection of the network access ports and SIP signaling interoperability with other untested network devices (clients, gateways, etc.).

1. Verify configuration of the proper network access port pairs (A1/A2, B1/B2) with the corresponding physical connections to network access switches.
2. Verify proper "network" and "server" side roles of the Ethernet interfaces. At the Linux CLI, verify the contents of the **/usr/local/ipcs/etc/ipcs310.cfg** file, an excerpt of which is shown below. The server-side interface information as it was entered during the installation CLI session is shown in bold. The other interface in the pair (B2/eth0) would be the network-side.

```
# IP Address configuration for bridge0
# IP Address of bridge1
# Call server
# Chat server
MGMT_IP=10.3.3.120
MGMT_SUBNET=255.255.255.0
MGMT_GW=10.3.3.1
MGMT_IFACE=eth4
BR0_IP=10.3.3.121
BR0_SUBNET=255.255.255.0
BR0_GW=10.3.3.1
CS_IP=10.3.3.60
CS_IFACE=eth1
```

3. Verify the IP addresses of protected servers using the **Network Configuration** -> **Call Server** menu in the web interface.
4. Verify that the protected and unprotected networks are reachable from bridge ports on the IPCS. Incoming pings are not supported on these ports for security and transparency reasons. Outgoing pings to the network can be used. In the case of the sample configuration, the following could be done from the serial console port, as shown below. Log in and enter super-user mode via the **su** command. Then start the IPCS command line interface via the **savon** command. The source interface for the **ping** command is the bridge **br0**.

```
login: ipcs
Password:
Last login: Thu Feb 23 16:24:29 from 10.3.3.119
[ipcs@avaya_ipcs ~]$ su –
Password:
[root@avaya_ipcs ~]# savon
Starting Savon Console...Please wait.
IPCS Version 2.1.0.Q06 (C) Sipera Systems Inc.
Savon Status:
Installation    Status
--------------- ----------------------------------------
sems            Running since Mar 10 13:57:13
si              Running since Mar 10 13:57:12
ss              Running since Mar 10 13:57:12
sv              Running since Mar 10 13:57:13
IPCS # ping -I br0 10.3.3.1
PING 10.3.3.1 (10.3.3.1) from 10.3.3.121 : 56(84) bytes of
data.
64 bytes from 10.3.3.1: icmp_seq=0 ttl=255 time=3.17 ms
64 bytes from 10.3.3.1: icmp_seq=1 ttl=255 time=1.19 ms
```

5. For troubleshooting purposes, the port bypass feature can be used to quickly compare the results of a particular SIP signaling scenario with and without the IPCS 310 in the network path. This feature can be manually enabled and disabled by using the **bypass enable** and **bypass disable** commands at the IPCS command line interface, as shown below. The status of the port bypass condition can be verified by using the **bypass status** command.

```
IPCS # bypass enable
IPCS # bypass status
Group A: Enabled
Group B: Enabled
IPCS # bypass disable
IPCS # bypass status
Group A: Disabled
Group B: Disabled
IPCS #
```

6. Support

For technical support on the Sipera Systems IPCS 310 email support@sipera.com or call (877) 275-1757.

7. Conclusion

The ability of the Sipera Systems IPCS 310 to interoperate with an Avaya SIP Telephony environment consisting of Avaya SIP Enablement Services, Avaya Communication Manager, Avaya 4600 Series SIP and IP Telephones, and Avaya SIP and IP Softphones has been successfully compliance tested.

8. References

The following documentation may be found at http://support.avaya.com:

[1] *Installing and Administering SIP Enablement Services R3.1*, Issue 1.4, Doc ID 03-600768, February, 2006.

[2] *Avaya Extension to Cellular and OPS Installation and Administration Guide*, Version 6.0 Issue 9, DocID 210-100-500, June 2005.

[3] *SIP Support in Release 3.1 of Communication Manager Running on the S8300, S8400, S8500, S8500B, S8700, and S8710 Media Server*, Issue 1.4, Doc ID 555-245-206, February, 2006.

[4] *Administrator Guide for Avaya Communication Manager*, Issue 2, Doc ID 03-300509, February 2006.

[5] *Configuring SIP IP Telephony Using Avaya SIP Enablement Services, Avaya Communication Manager, and Cisco 7940/7960 SIP Telephones - Issue 1.1*.

Additional Documentation:

[6] *IPCS 310 Product Guide*, Release 2.1, Sipera Systems, Part Number: 310-5100-21, January 2006, available with the shipped product or from the support area on www.sipera.com (login/password required).

[7] *Session Initiation Protocol Service Examples - draft-ietf-sipping-service-examples-06*, SIPPING Working Group, Internet-Draft, 2/15/2004, available at http://tools.ietf.org/wg/sipping/draft-ietf-sipping-service-examples/draft-ietf-sipping-service-examples-10.txt.

The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya Developer*Connection* Program at devconnect@avaya.com.