



Avaya Solution & Interoperability Test Lab

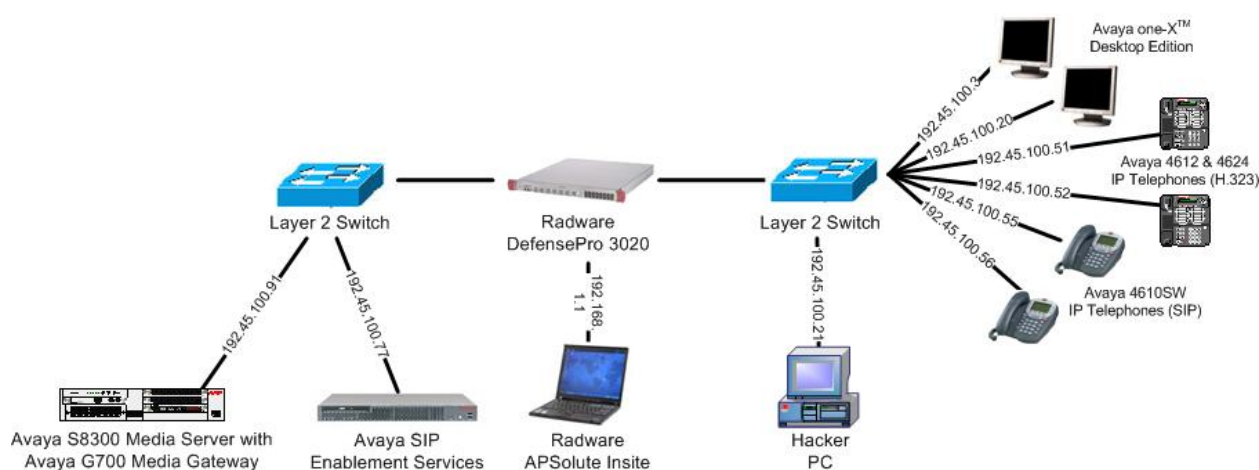
Application Notes for Configuring Radware DefensePro 3020 in an Avaya SIP Telephony Environment – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for the Radware DefensePro 3020 security appliance to successfully interoperate in an Avaya SIP Telephony environment consisting of Avaya Communication Manager, Avaya SIP Enablement Services, Avaya 4600 Series H.323 and SIP Telephones, and Avaya one-X™ Desktop Edition. Information in these Application Notes has been obtained through compliance testing and additional technical discussions. Testing was conducted via the *DeveloperConnection* Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

The Radware DefensePro 3020 is an intrusion prevention and denial of service protection solution that protects against network, operating system, and application level attacks from worms, viruses, hackers, SYN floods and other DoS attacks. Both known and unknown zero-day attacks can be blocked by DefensePro 3020's adaptive self-learning behavior-based capabilities. The DefensePro 3020 provides multi-layer security by integrating content signature-based, behavior-based and rate-based protection into a single multi-layer-security solution, and features inline security switching and stateful packet inspection to bi-directionally scan and protect all network traffic.



As shown in the above configuration, the Radware DefensePro 3020 is configured to protect the Avaya servers from the security attacks. The Avaya servers include the Avaya SIP Enablement Services server, and the Avaya S8300 Media Server running Avaya Communication Manager with Avaya G700 Media Gateway. The two Layer 2 switches are connected to a pair of static forwarding ports on the DefensePro 3020. The Radware APSolute Insite is an application that provides the main management interface for all Radware devices, including the DefensePro 3020. The APSolute Insite is used to configure, modify, and manage the DefensePro 3020.

For the compliance testing, various security attacks were launched from the Hacker PC. Upon detecting an attack, DefensePro 3020 prevents propagation by executing the predefined action in the security policy, while continuing to inspect and forward the legitimate application traffic between the pair of static forwarding ports. DefensePro 3020 also has an internal bypass mode that can be triggered upon a power failure or shut down of the DefensePro 3020 application, such that the pair of static forwarding ports can continue to forward traffic to one another without DefensePro 3020 software services.

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

2. Equipment and Software Validated

The following equipment and software were used for the sample configuration provided:

Equipment	Software
Avaya S8300 Media Server with G700 Media Gateway	Communication Manager 3.1.1, load 628.7
Avaya SIP Enablement Services	3.1, load 18
Avaya 4612 & 4624 IP Telephones (H.323)	1.8.3
Avaya 4610SW IP Telephones (SIP)	2.4
Avaya one-X™ Desktop Edition	2.1, build 44
Radware DefensePro 3020	3.00.00
Radware APSolute Insite running on IBM ThinkPad with Windows XP Professional	2.00 V2002 SP2
Hacker PC	Red Hat Enterprise Linux ES 3

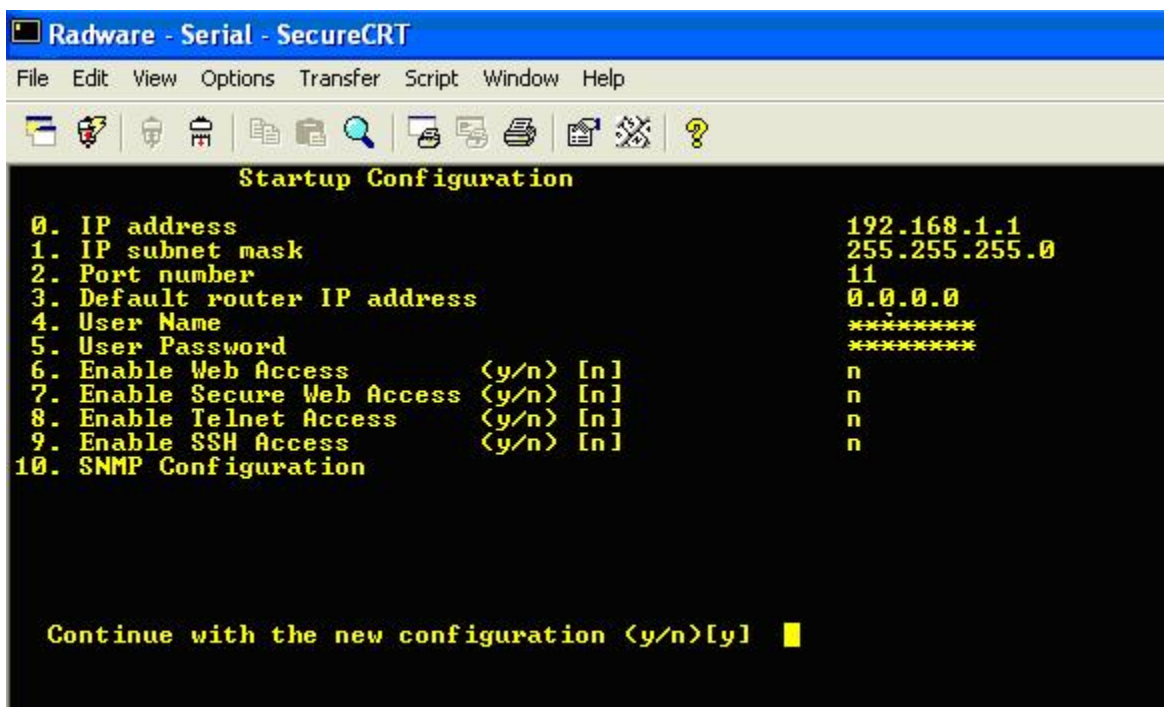
3. Configure Radware DefensePro 3020

This section provides the procedures for configuring Radware DefensePro 3020. The procedures include the following areas:

- Administer IP address and management port
- Administer device
- Administer security policy

3.1. Administer IP Address and Management Port

Connect a PC to the console serial port of the DefensePro 3020. The **Startup Configuration** screen is displayed. Enter an **IP address**, **IP subnet mask**, and **Port number** that will be used for APSolute Insite connectivity, as shown below. Default values of remaining fields may be modified as necessary. Consult the Radware documentation listed in **Section 8** for detailed descriptions. For the compliance testing, default values were retained for all remaining fields. Press the <Enter> key to continue with the new configuration.



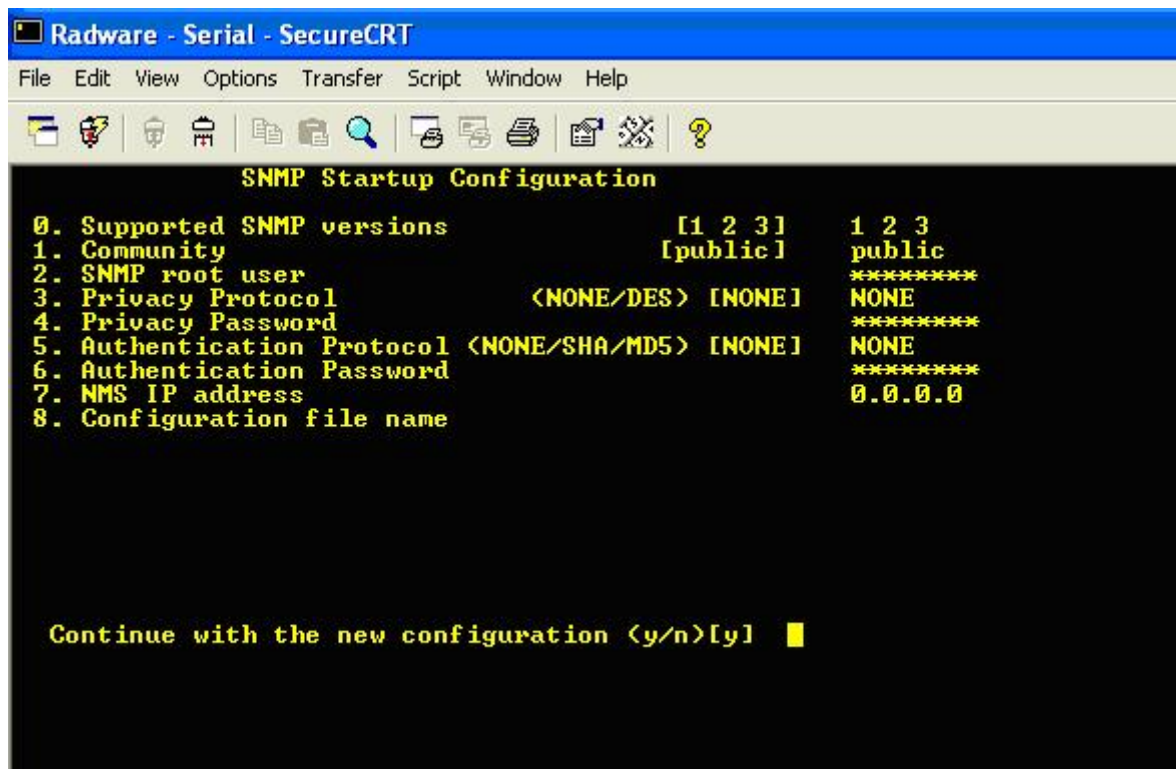
```
Radware - Serial - SecureCRT
File Edit View Options Transfer Script Window Help

Startup Configuration

0. IP address 192.168.1.1
1. IP subnet mask 255.255.255.0
2. Port number 11
3. Default router IP address 0.0.0.0
4. User Name *****
5. User Password *****
6. Enable Web Access (y/n) [n] n
7. Enable Secure Web Access (y/n) [n] n
8. Enable Telnet Access (y/n) [n] n
9. Enable SSH Access (y/n) [n] n
10. SNMP Configuration

Continue with the new configuration (y/n)[y]
```

The **SNMP Startup Configuration** screen is displayed next. Field default values may be modified as necessary. Consult the Radware documentation listed in **Section 8** for detailed descriptions. For the compliance testing, all default values were retained. Press the <Enter> key to continue with the new configuration.



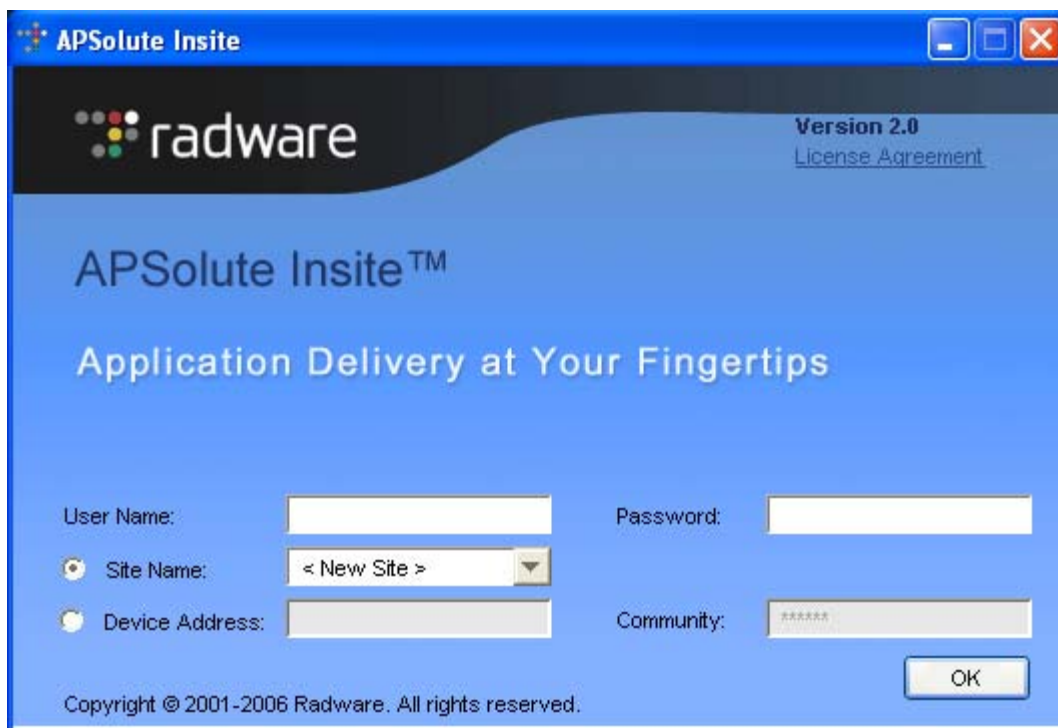
The **Startup Configuration** screen shown previously is displayed again, to provide the user an opportunity to make any additional changes. Accept all displayed values.

3.2. Administer Device

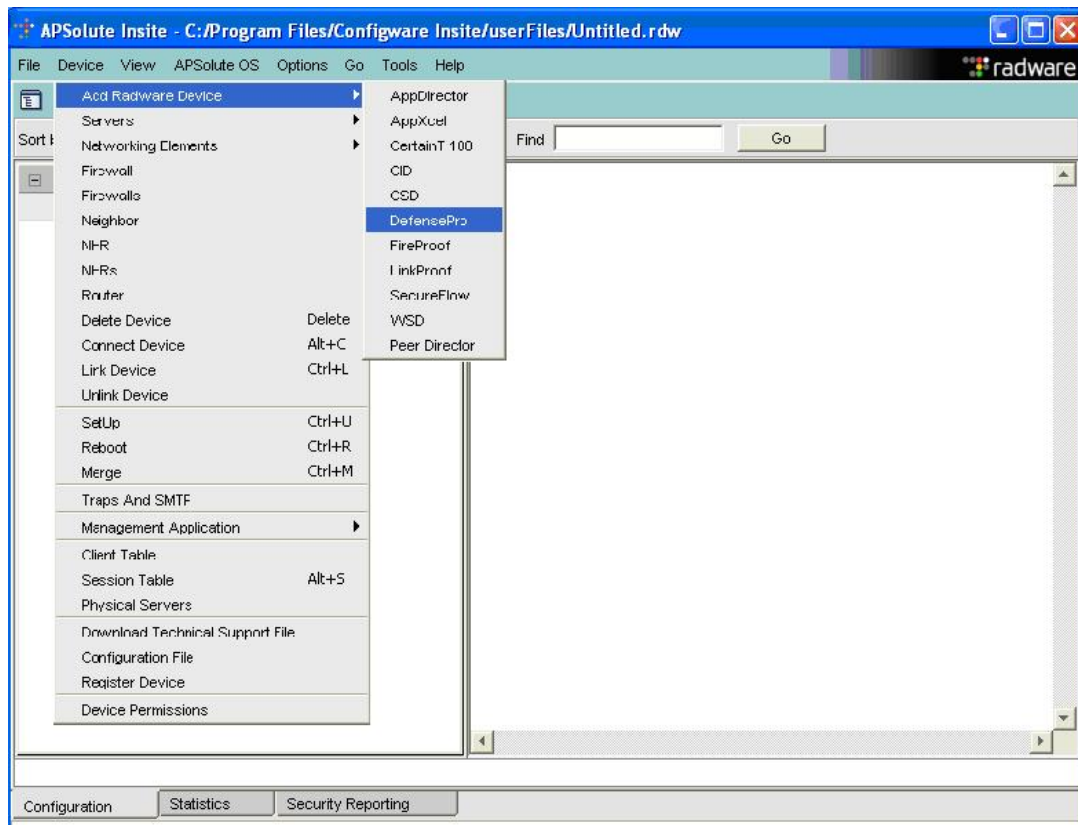
Physically connect the PC running the APSolute Insite application to the DefensePro 3020 management port. For the compliance testing, the physical port chosen as the management port was “11”, as configured in **Section 3.1**. Double click on the **APSolute Insite** icon below from the PC to launch the application.



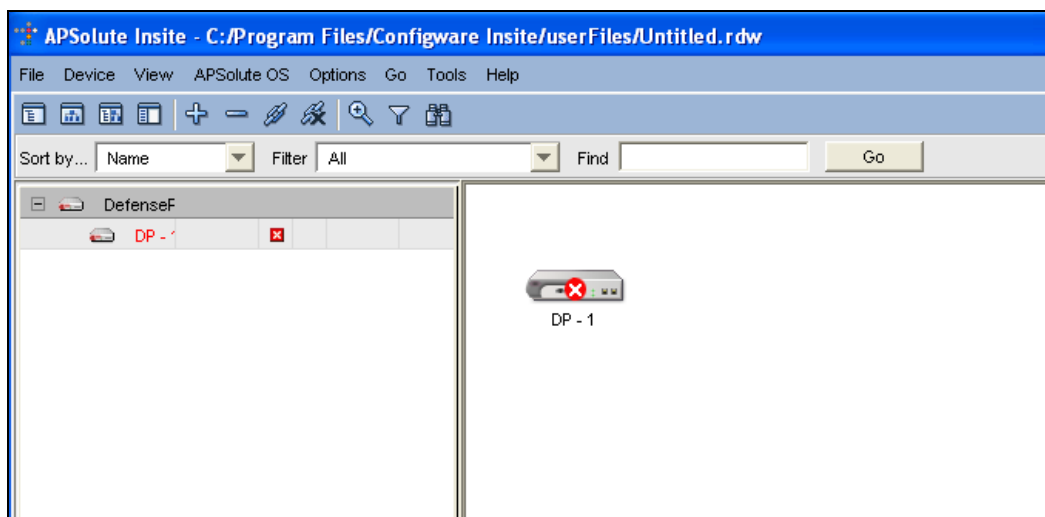
The following **APSolute Insite login** screen is displayed. For **User Name** and **Password**, enter the corresponding values from **Section 3.1**. Click **OK**.

The login screen for APSolute Insite has a blue background. At the top left is the "radware" logo. At the top right, it says "Version 2.0" and has a link for "License Agreement". The main title "APSolute Insite™" is in the center, with the tagline "Application Delivery at Your Fingertips" below it. The login fields are arranged in two columns. The first column has "User Name:" followed by a text box, "Site Name:" followed by a dropdown menu showing "< New Site >", and "Device Address:" followed by a text box. The second column has "Password:" followed by a text box, "Community:" followed by a text box with masked characters, and an "OK" button at the bottom right. A copyright notice "Copyright © 2001-2006 Radware. All rights reserved." is at the bottom left.

The following **APolute Insite main** screen is displayed next. Select **Device > Add Radware Device > DefensePro** from the menu drop down lists as shown below.



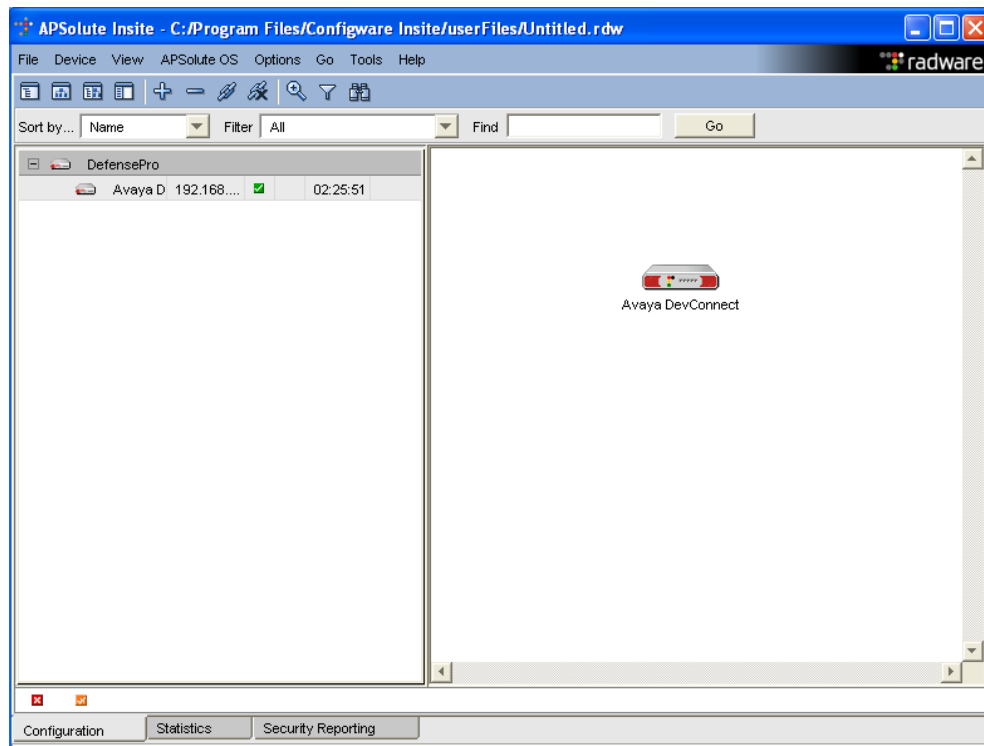
The **APolute Insite main** screen is updated with a **DP-1** icon displayed into the right pane. Double click on the **DP-1** icon.



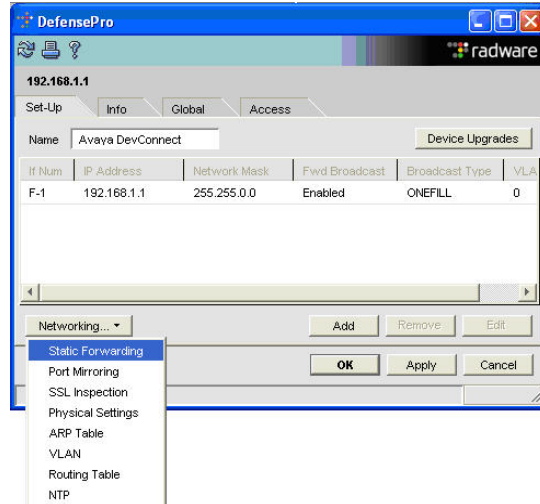
The **Connect DP Device** dialog box is displayed. For the **Device IP Address** field, enter the **IP address** from **Section 3.1**, in this case “192.168.1.1”. For the **Device Community Name**, enter a descriptive name, in this case “Avaya DevConnect”. Click **OK**.



The **APSolute Insite main** screen is updated with the IP address and device name as shown below. Double click on the **Avaya DevConnect** icon in the right pane.



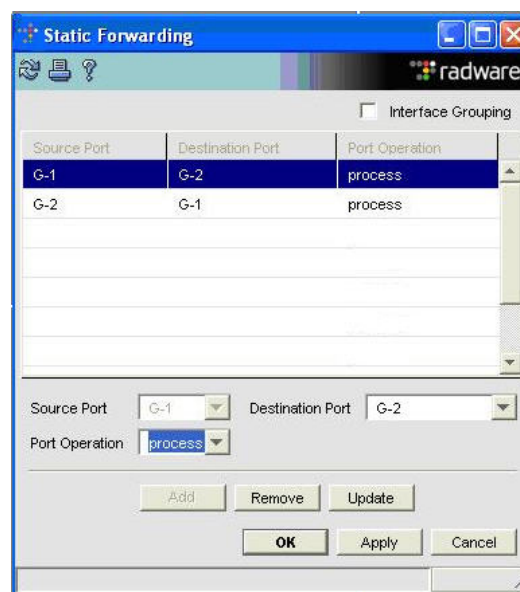
The **DefensePro** screen appears. Right click on **Networking** and select **Static Forwarding**.



The **Static Forwarding** screen is displayed, and used to administer the pair of static forwarding ports. For each traffic direction, create a new entry in the table with the following values:

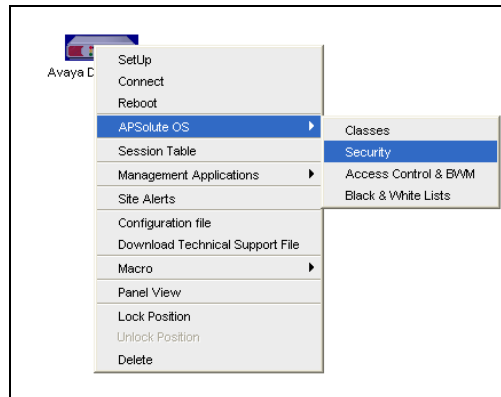
- **Source Port:** Select the source port for received traffic.
- **Destination Port:** Select the destination port for transmitted traffic.
- **Port Operation:** Select “process” to enable packet inspection.

For the compliance testing, the Avaya telephones and hacker PC are connected to port “G-1”, and the Avaya servers are connected to port “G-2”. Traffic from both directions is inspected with the “process” option in the **Port Operation** field for a more strenuous test. Note that the “forward” option could have been used from port G-2 to G-1 to allow straight forwarding of packets from the Avaya servers. Click **OK** to submit the changes.



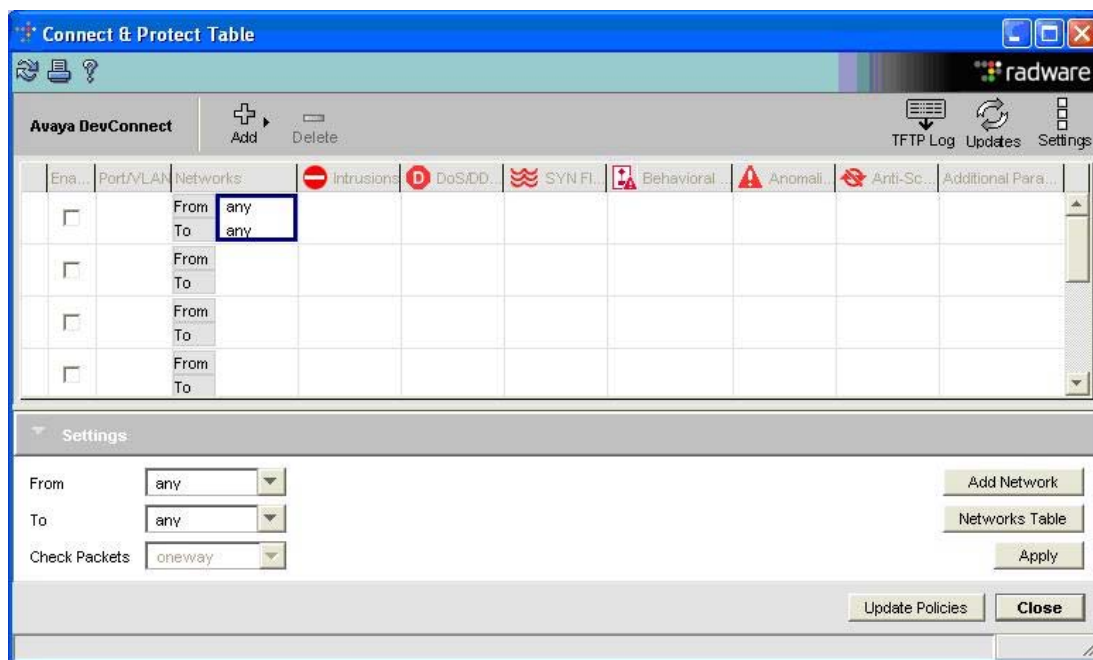
3.3. Administer Security Policy

From the **APSolute Insite** main screen, right click on the **Avaya DevConnect** icon in the right pane, and select **APSolute OS > Security** from the drop down lists.



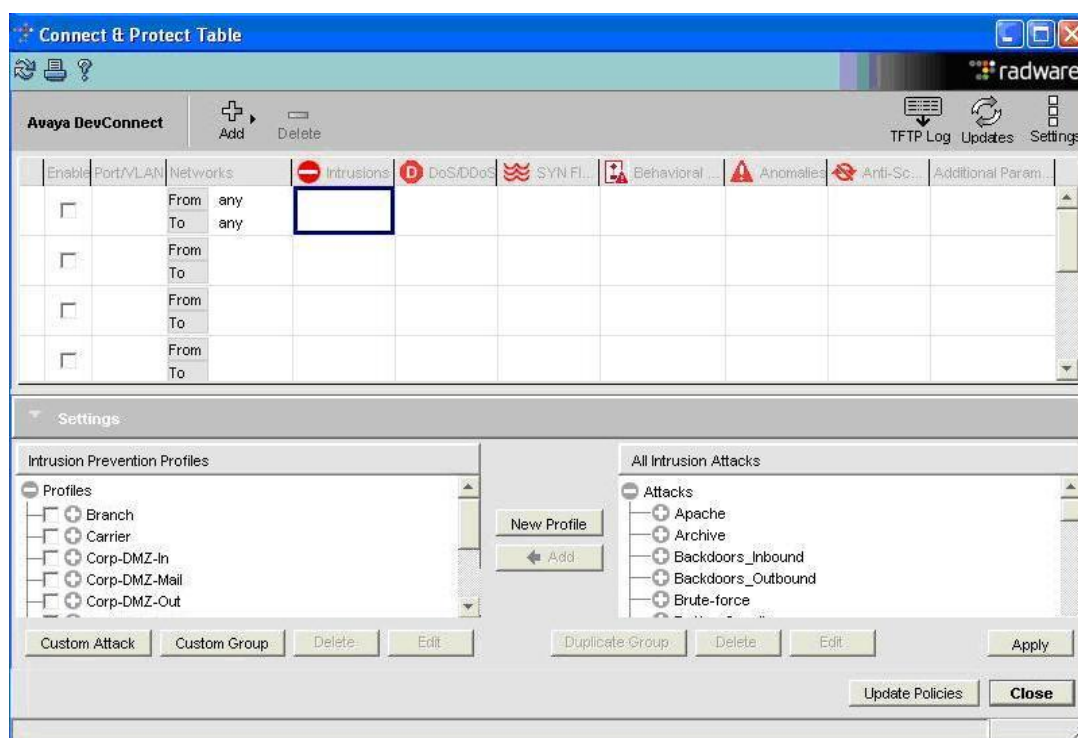
The **Connect & Protect Table** screen is displayed. This table is used to define security policies for the system. Create a new security policy by clicking on the first blank grid under the **Networks** column, and the associated parameters are displayed into the **Settings** pane. Select “any” from the drop down lists for the **From** and **To** fields in the **Settings** pane, to enable the security policy to be applied to all source and destination networks in the system. Click on **Apply**.

For the compliance testing, the new security policy is configured to apply to the entire system. Customers can limit each security policy to specific ports and VLANs by using the **Port/VLAN** field to define the applicable ranges.

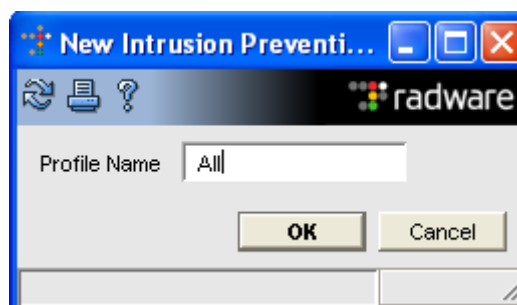


3.3.1. Administer Intrusion Protection

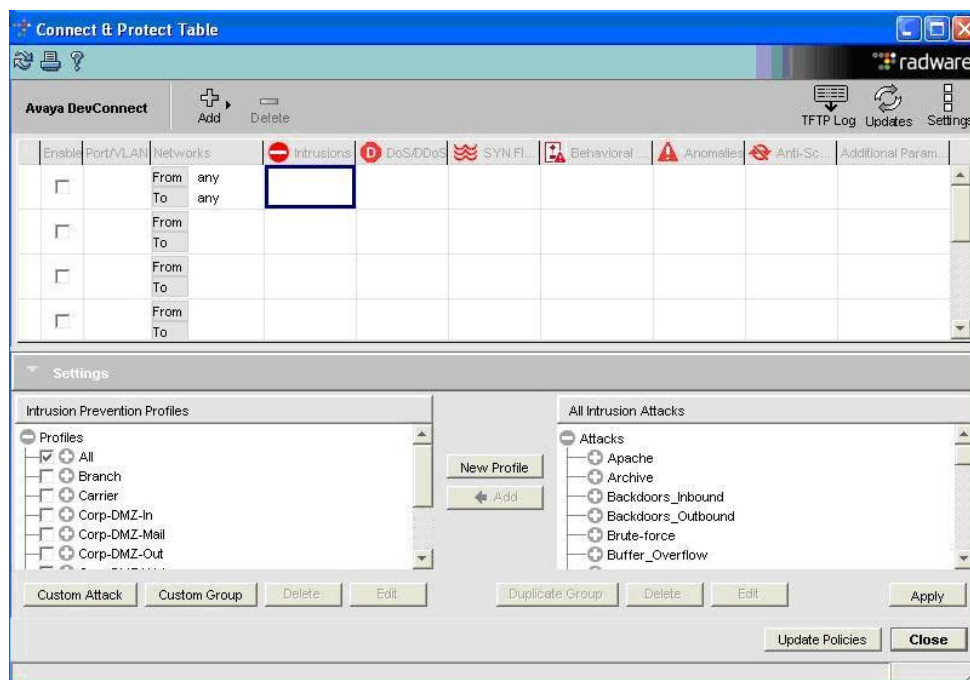
From the **Connect & Protect Table** screen, double click on the corresponding grid in the **Intrusions** column for the security policy, to display the **Settings** pane. The **Intrusion Prevention Profiles** area displays a list of pre-defined profiles, and the **All Intrusion Attacks** area provides a list of pre-defined types of intrusion attacks. The user can consult the Radware documentation for selecting the appropriate profile and intrusion attacks to correspond to the network configuration, or create a new profile with pre-defined and user defined types of attacks. For the compliance testing, a new profile is created to contain all pre-defined types of intrusion attacks. Click on **New Profile**.



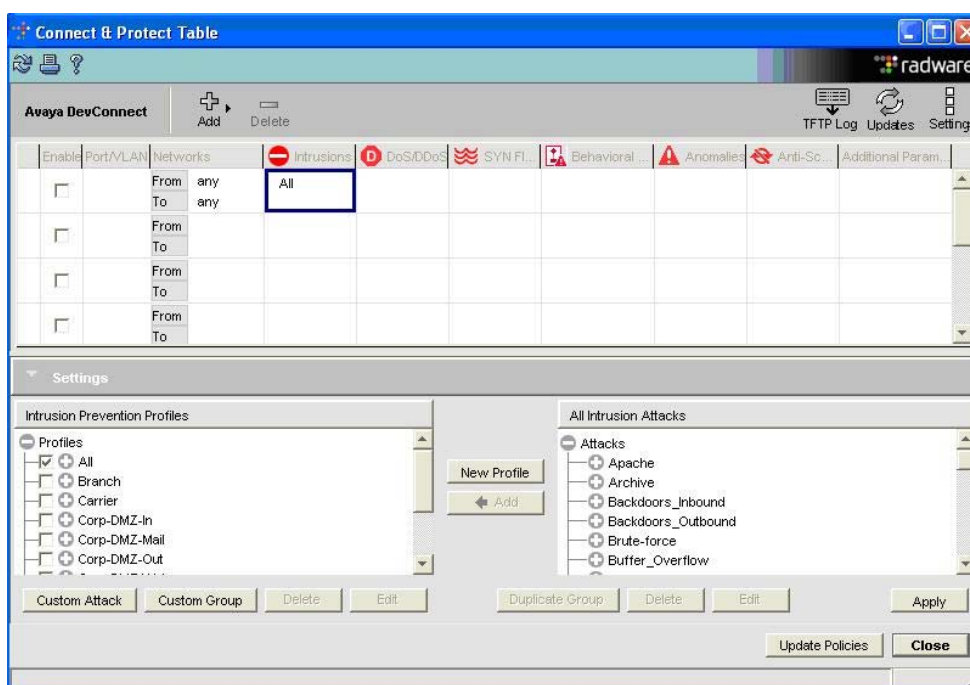
The **New Intrusion Prevention** dialog box is displayed. Enter a descriptive **Profile Name**, and click **OK**.



The **Intrusion Prevention Profiles** pane is updated with the newly created profile. Check the newly created profile in the **Intrusion Prevention Profiles** section, and apply all pre-defined intrusion attacks by selecting each group of attacks in the **All Intrusion Attacks** section followed by the leftward arrow.

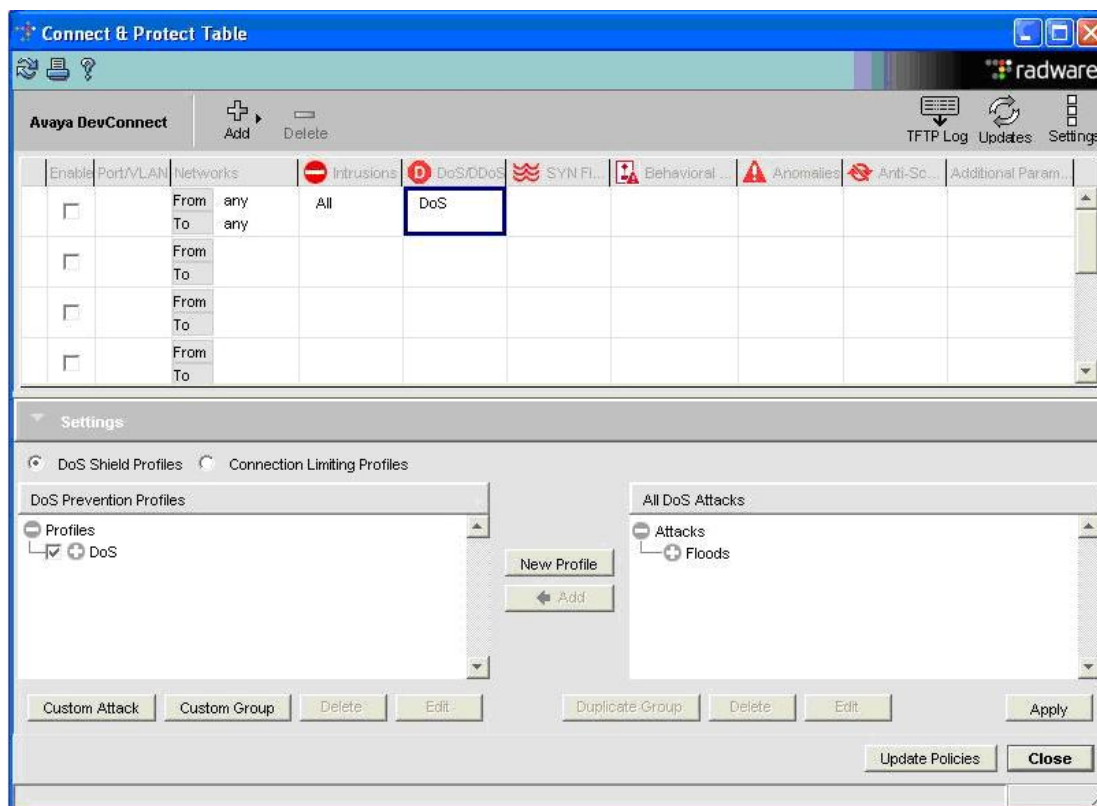


Apply the newly created intrusion profile to the security policy by clicking on the corresponding grid in the **Intrusions** column, followed by the **Apply** button at the bottom right of the screen.



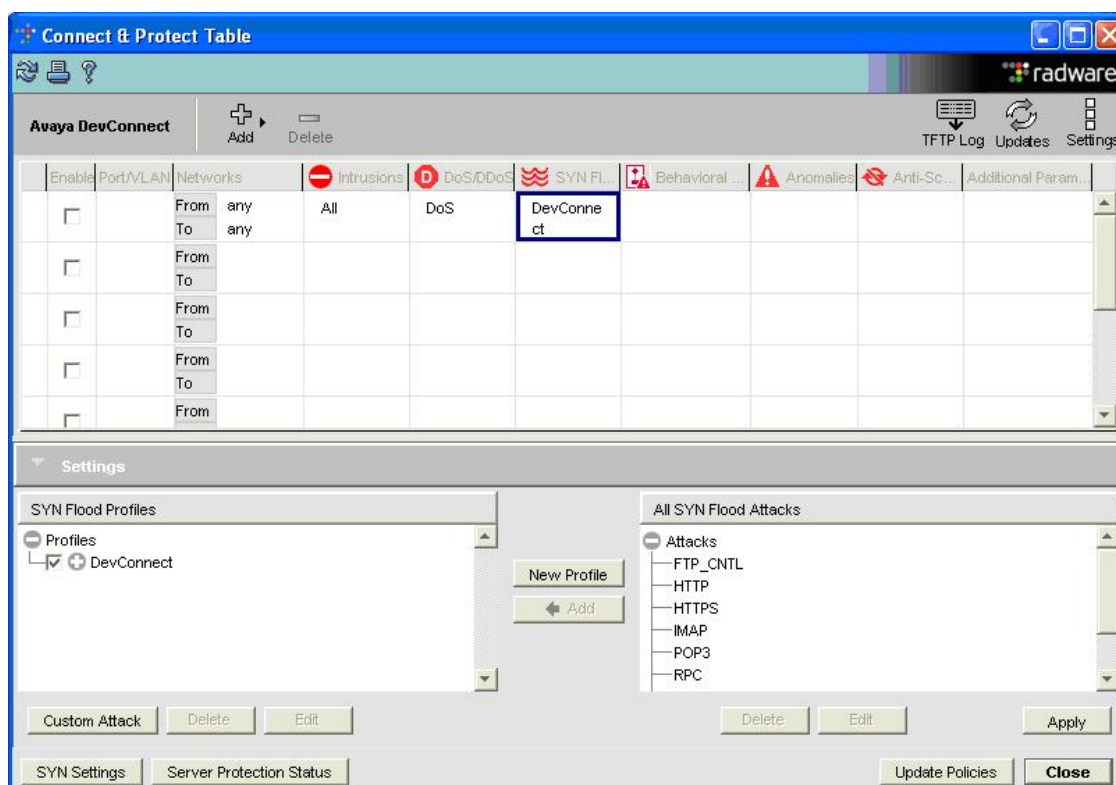
3.3.2. Administer DoS or Distributed DoS Protection

From the **Connect & Protect Table** screen, double click on the corresponding grid in the **DoS/DDoS** column for the security policy, to display the **Settings** pane. The procedures for creating a new DoS/DDoS profile with all pre-defined DoS attacks are similar to the creation of the intrusion profile. Follow the procedures described in **Section 3.3.1** to create the new “DoS” profile shown below.

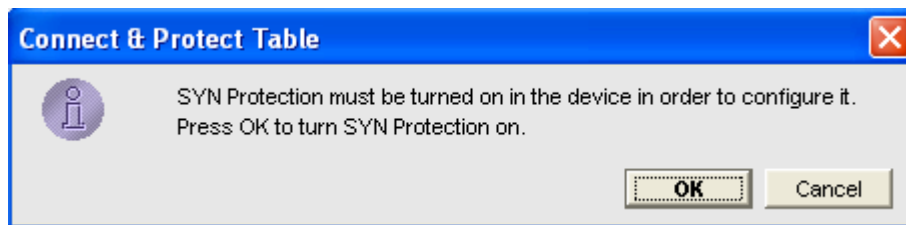


3.3.3. Administer SYN Flood Protection

From the **Connect & Protect Table** screen, double click on the corresponding grid in the **SYN Flood** column for the security policy, to display the **Settings** pane. The procedures for creating a new SYN flood profile with all pre-defined SYN flood attacks are similar to the creation of the intrusion profile. Follow the procedures described in **Section 3.3.1** to create the new “DevConnect” profile shown below.

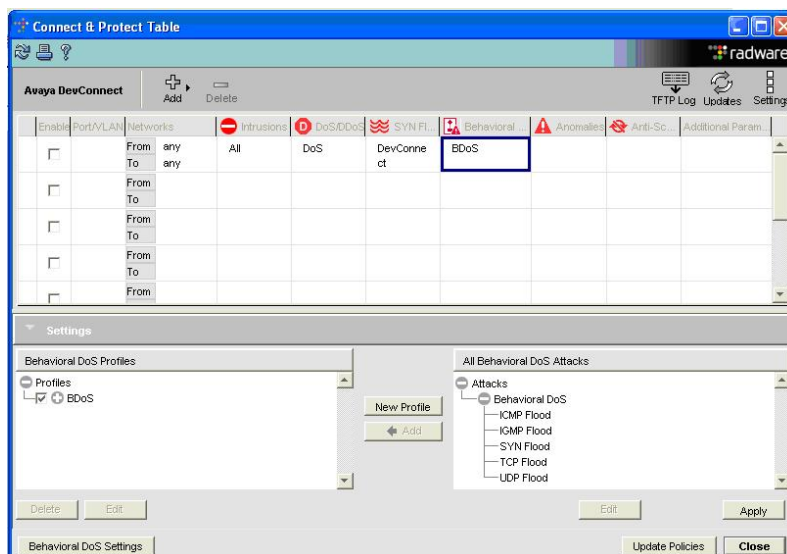


Upon clicking the **Apply** button, the following dialog box is displayed. A reboot of the system is necessary to create the table and allocate the memory for SYN flood protection. Click **OK** to proceed with the device reboot.



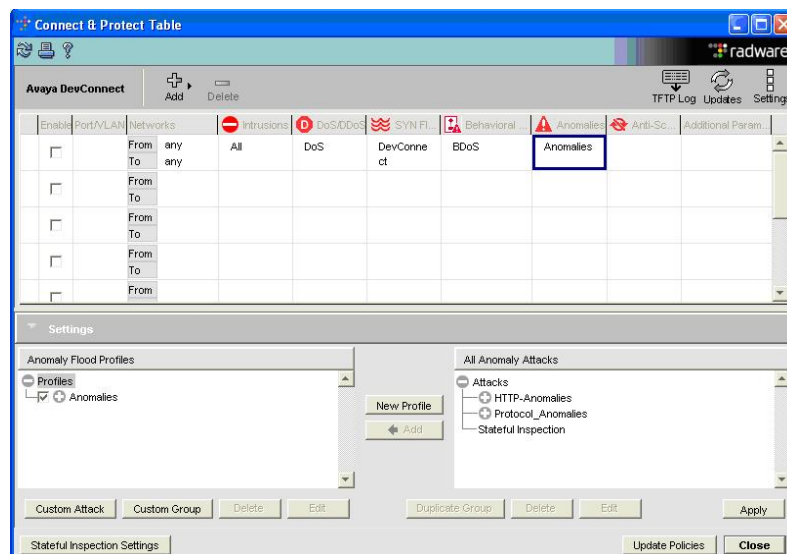
3.3.4. Administer Behavioral DoS Protection

From the **Connect & Protect Table** screen, double click on the corresponding grid in the **Behavioral DoS** column for the security policy, to display the **Settings** pane. The procedures for creating a new behavioral DoS profile with all pre-defined behavioral DoS attacks are similar to the creation of the intrusion profile. Follow the procedures described in **Section 3.3.1** to create the new “BDoS” profile shown below.



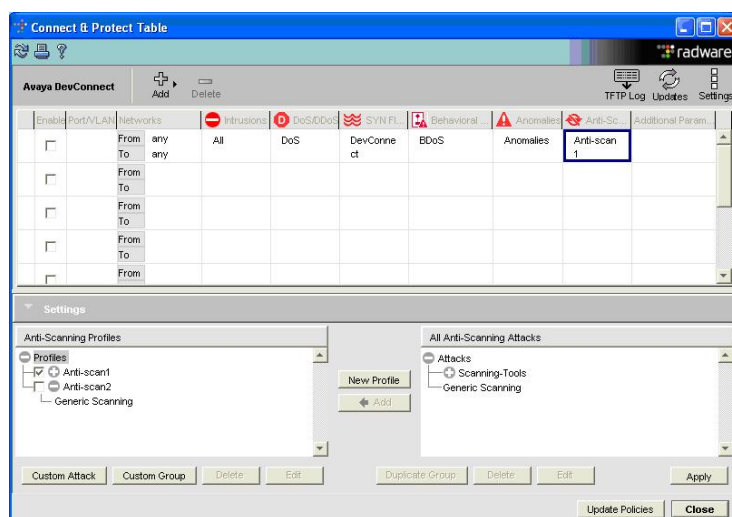
3.3.5. Administer Anomalies Protection

From the **Connect & Protect Table** screen, double click on the corresponding grid in the **Anomalies** column for the security policy, to display the **Settings** pane. The procedures for creating a new anomalies profile with all pre-defined behavioral anomaly attacks are similar to the creation of the intrusion profile. Follow the procedures described in **Section 3.3.1** to create the new “Anomalies” profile shown below.



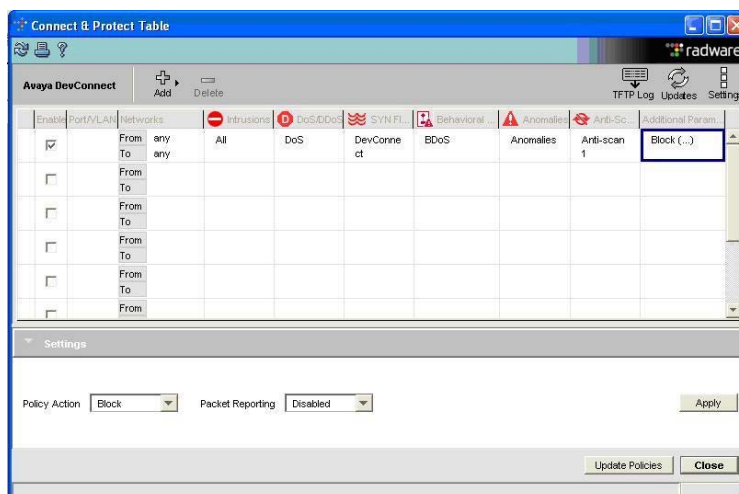
3.3.6. Administer Anti-Scanning Protection

From the **Connect & Protect Table** screen, double click on the corresponding grid in the **Anti-Scanning** column for the security policy, to display the **Settings** pane. The procedures for creating a new anti-scanning profile with all pre-defined anti-scanning attacks are similar to the creation of the intrusion profile. Follow the procedures described in **Section 3.3.1** to create the new “Anti-scan1” profile shown below.



3.3.7. Administer Additional Parameters

From the **Connect & Protect Table** screen, double click on the corresponding grid in the **Additional Parameters** column for the security policy, to display the **Settings** pane. For the **Policy Action** field, select “Block” to enable dropping of security attack packets upon detection. Keep the default value for the **Packet Reporting** field. Click **Apply**.



Activate the new security policy by checking the corresponding grid in the **Enable** column, followed by **Update Policies**.

4. Interoperability Compliance Testing

The interoperability compliance test included security attacks, SIP features, and serviceability testing.

The security attacks testing included ping floods (used and unused IP addresses), SYN/ICMP floods, port scans (vertical and horizontal), TCP/TLS/UDP port attacks, and H323/SIP registration attacks. The security attacks focused on attacking the Avaya servers.

The feature testing included basic SIP features of registration, basic calling, hold, transfers, conference, call forwarding, bridging, presence, and instant messaging. The focus is on verifying these basic SIP features continue to work while the system is under security attack.

The serviceability testing focused on verifying the ability of DefensePro 3020 to trigger the internal bypass mode upon pulling the power cord, such that the IP traffic can continue to be forwarded between the two static forwarding ports without the DefensePro 3020 application.

4.1. General Test Approach

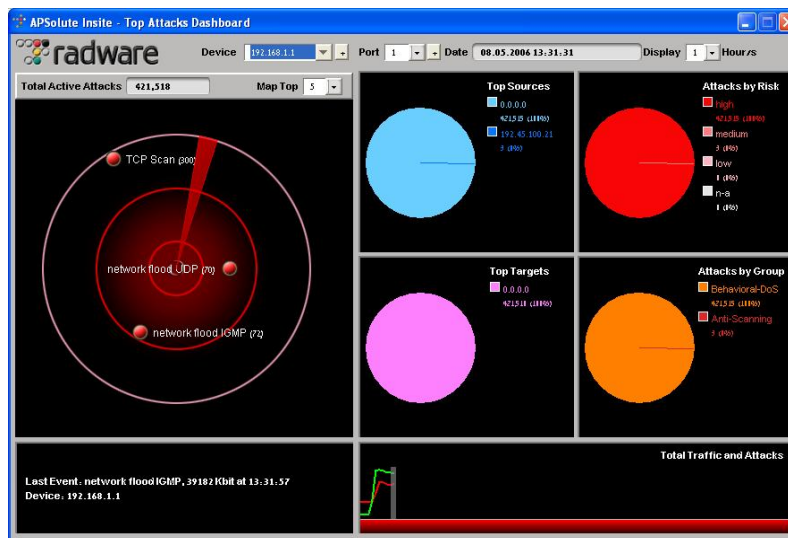
All tests were performed manually. Various forms of security attacks were verified to be detected, logged, and blocked by DefensePro 3020, with detailed descriptions provided in the attack logs. While the system was under attack, the feature test cases were executed to verify that the legitimate traffic continued to flow through.

4.2. Test Results

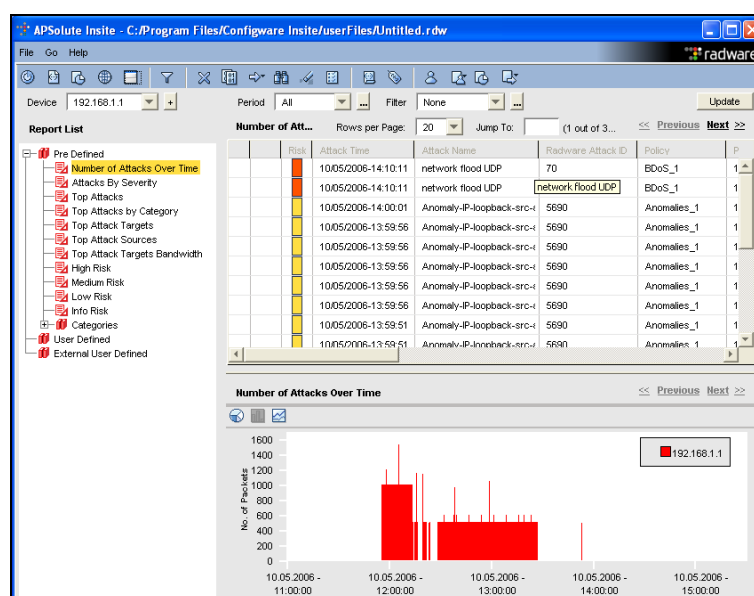
All test cases were executed and passed.

5. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Radware DefensePro 3020. Launch a security attack from the hacker PC to one of the Avaya servers. From the **APSolute Insite** main menu screen, click on the **Security Reporting** tab at the bottom of the screen. Double click on the dashboard icon (not shown) to bring up the **APSolute Insite - Top Attacks Dashboard** screen below. This real-time monitoring tool displays the most intensive attacks currently in the system. Verify that the newly launched attack is detected and displayed in the radar screen.



From the **APSolute Insite** main menu screen, click on the **Security Reporting** tab at the bottom of the screen. Double click on the logs icon (not shown) to bring up the logs screen below. Verify that the details of the newly launched attack are displayed in the logs.



6. Support

Technical support on Radware DefensePro 3020 can be obtained through the following:

- **Phone:** (877) 236-9807
- **Email:** support@radware.com

7. Conclusion

These Application Notes describe the configuration steps required for Radware DefensePro 3020 Release 3.00 to successfully interoperate with an Avaya SIP Telephony environment consisting of Avaya Communication Manager 3.1, Avaya SIP Enablement Services 3.1, Avaya 4600 Series IP Telephones, and Avaya one-XTM Desktop Edition.

8. Additional References

This section references the product documentation relevant to these Application Notes.

- *Administrator Guide for Avaya Communication Manager*, Document 03-300509, Issue 2, February 2006, available at <http://support.avaya.com>.
- *Installing and Administering SIP Enablement Services R3.1*, Document ID 03-600768, Issue 1.4, February 2006, available at <http://support.avaya.com>.
- *SIP Support in Release 3.1 of Avaya Communication Manager Running on the S8300, S8400, S8500 series, and S8700 series Media Server*, Document 555-245-206, Issue 6, February 2006, available at <http://support.avaya.com>.
- *DefensePro 3.00 User Manual*, Software Version 3.00, March 2006, available at <http://www.radware.com> with proper login.
- *VoIP Security Threats and Solutions*, available at <http://www.radware.com> with proper login.
- *DefensePro Best Practices for Transparent Introduction*, available at <http://www.radware.com> with proper login.
- *Radware's Security Zone*, available at <http://www.radware.com> with proper login.

©2006 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. 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.