



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"
at <http://www.giac.org/registration/gsec>

**Who's knocking on the door:
Using Securify SecurVantage to monitor the outside of
the security perimeter.**

Phillip R. Hammond Jr.

**GIAC Security Essentials Certification (GSEC)
Practical Assignment
Version 1.4b, Option 1
February 7, 2004**

© SANS Institute 2004, Author retains full rights.

Table of Contents

1. Overview	2
2. Why Monitor the Outside?	3
3. About Securify, Inc. and the SecurVantage Products	4
A. Company Information.....	4
B. SecurVantage Overview	4
C. SecurVantage Monitor	4
D. SecurVantage Monitor LE.....	5
E. SecurVantage Enterprise Manager.....	5
F. SecurVantage Enterprise Reporter	5
G. SecurVantage Studio.....	5
H. Security of the SecurVantage Product Suite.....	5
4. Information Gathering and Preparation	6
A. Information required to configure the monitor	6
B. Example network information for this document	7
C. Preparation	8
5. Equipment Installation and Configuration.....	9
A. Hardware installation	9
B. Install the Monitor software	9
C. Verify connectivity	10
D. Some Details on Policy Development.....	11
E. Policy development.....	16
F. Policy installation	26
G. Policy refinement	27
6. SecurVantage Monitor Web Interface	33
7. Evaluating Results	34
A. General	34
B. Summary IP Query	34
C. Getting data out of Securify.....	35
8. Summary.....	35
9. References.....	36

© SANS Institute 2004. All rights reserved. Author retains full rights.

Table of Figures

Figure 1 – Yourco Network Diagram	7
Figure 2 - Monitor LE Connections.....	9
Figure 3 - Web Interface Login Page.....	10
Figure 4 - Web Interface Home Page.....	10
Figure 5 – Adding a Rule to a Host	12
Figure 6 – Adding a Service.....	13
Figure 7 – Defining a New Outcome	14
Figure 8 – SQOS Settings	15
Figure 9 – Initial Blank Policy	16
Figure 10 – Save Dialog Box	16
Figure 11 – First Subnet	17
Figure 12 – First Subnet Detail Dialog Box.....	17
Figure 13 – Beginning Firewall 2 Path.....	18
Figure 14 – Firewall 2 Objects	19
Figure 15 – Firewall 2 Path with Connectors	20
Figure 16 – Both Firewall Paths	21
Figure 17 – Complete Policy Diagram	22
Figure 18 – DMZ Web Server Addressing.....	22
Figure 19 – Before and After Adding the DMZ Subnet Address	23
Figure 20 – Inside Hosts Grouped Automatically.....	23
Figure 21 – Connection List Dialog Box	27
Figure 22 – Analyzer Connection Dialog Box	27
Figure 23 – Initial Analyzer Workbook	28
Figure 24 – Initial Analyzer Workbook	29
Figure 25 – Sort by Criticality and Count	30
Figure 26 – Refine Policy in Workbook	31
Figure 27 – Web Interface Home Page.....	33
Table 1 – Initial Rules	24
Table 2 – Analyzer Buttons.....	28

1. Overview

Are your security policies, procedures and equipment really working? How can you tell? Securify SecurVantage products are designed to monitor your network and determine if your traffic complies with your policies. SecurVantage can be installed outside your security perimeter and allows you to see what is being turned away by your security as well as what is getting in and out of your network. It will also assist in finding chinks in the armor that you thought was closed.

The Securify SecurVantage product suite has many uses. I will not attempt to cover all of the products or all of the uses in this document, but an overview of the product suite is included. This paper will primarily discuss how to configure Securify Monitors to monitor traffic traversing the security perimeter of an example network. It will show the basics of how to install and configure the equipment, develop and install a policy, and monitor the results. Since the Securify software is not available in the public domain, I will include screen shots to help illustrate the procedures.

Note: Securify recently released Version 4 of the SecurVantage product suite, but this document is based on the Version 3 product. The features that are discussed here are still available in version 4, and some new features have been added. Some of the details of the interfaces have changed between Version 3 and version 4, so some of the procedures detailed in this document will be slightly different in Version 4.

2. Why Monitor the Outside?

Most security efforts take place inside the network, and stop at the outside router. The area outside of the outermost router is a no man's land that rarely gets examined. Good security practice dictates logging events from the perimeter security devices to assist in determining what happened, as well as generating alerts when something out of the ordinary happens. The result, aptly described by Steven Scott, is that the average Security Manager in a medium to large company "is overwhelmed with large amounts of log information and bombarded with alerts". (Scott, p.3) Most Security Managers trust that their outside router is rejecting the traffic it has been told to reject, and do not have a secure method to verify that belief. Securify SecurVantage monitors are secure enough to deploy outside the normal security perimeter.

With SecurVantage, security architects are assured their security policies are in effect across the network, network administrators can easily confirm their security implementations are correct, and business managers have confidence their business practices are being effectively executed and they are getting a return on their security investments. ("Securify", PR Newswire)

In an ideal deployment of defense in depth, a security perimeter should have several layers at each network egress point. From a hardware perspective, these layers typically consist of an Outside Security Screening Router, a Firewall, and an Inside Security Screening Router. This hardware may be performing NAT, proxy services or other security procedures. In order for information to penetrate into the trusted network, it must traverse each layer of the security perimeter. However, in many cases, the failure to penetrate may be revealing to someone attempting to probe your defenses. Monitoring your network traffic from the outside allows visibility of what does traverse the perimeter, and also allows observation of failed attempts to penetrate your security.

Who is knocking on your door?

© SANS Institute 2004

3. About Securify, Inc. and the SecurVantage Products

A. Company Information

Securify, headquartered in Mountain View, CA, is a privately held company that provides Network security management products. The company delivers products that allow their clients to measure the effectiveness of their network security and have an unprecedented view of what is happening on their network in real time. Securify was founded by Dr. Taher Elgamal, who was responsible for the development of SSL, among other security contributions. (Securify)

B. SecurVantage Overview

From the ITsecurity.com article "Securify Scales SecurVantage to the Next Level":

Securify SecurVantage consists of Securify SecurVantage Studio, the policy development and analysis environment; Securify SecurVantage Monitor, the monitoring and compliance system; and Securify SecurVantage Enterprise, which aggregates and analyzes relevant data across an enterprise and presents it in a variety of reports. Using SecurVantage, enterprises can specify a formal set of requirements network traffic must comply with -- a "policy" describing the "correct" behavior of the network -- based on corporate security policy and industry best practices. Using these requirements, SecurVantage continuously evaluates, in real time, the packets moving across the network at all levels of the protocol stack, and makes decisions as to whether or not the traffic is consistent with the policy. This information is then clearly presented in a Web-based analysis environment in a format appropriate to the specific business. (ITsecurity)

"SecurVantage is distinguished from other products because it can identify application layer traffic, specific servers and users on the network. The product uses policies to flag unauthorized traffic. Because the product does not affect network traffic—in other words, SecurVantage does not make new policies for firewalls or routers—it does not interfere with new traffic". (Sturdevant, eWeek)

C. SecurVantage Monitor

The SecurVantage Monitor consists of a pair of 1U rack mount servers for high bandwidth situations. The Monitor is designed to connect to Gigabit Ethernet, and can handle up to 800 megabits per second of sustained throughput. Each system has two 10/100/1000 copper Ethernet ports, and they use a short cross-over cable to connect to each other. The cable is required, and provides a secure communications channel between the two parts of the Monitor. Using a fiber to copper adapter, Monitors can be deployed in a Gigabit fiber environment.

The first server in a Monitor installation is called the Harvester, and it does the low level work. The Harvester uses its available Ethernet port in promiscuous mode to collect real time network traffic. It can be connected to a mirror port on a switch or to a hub inserted between two network devices. The Harvester strips the payload from the packets and assembles the network events into DME files. A DME file uses a Securify proprietary file format to store event data. The DME files get passed, via the dedicated interface, to the Security Master.

The second server in a Monitor installation is the Security Master. This unit evaluates the data received from the Harvester against the policy and stores the results

in the local Sybase database. If the traffic is acceptable, the Security Master stores statistics in the database. If not, the event details get stored in the database. The available Ethernet port on this unit is the Management interface, which requires an IP address. The Management interface is used for real-time monitoring and remote management via SSL connections.

D. SecurVantage Monitor LE

The Monitor LE is a single 1U rack mount server for lower bandwidth situations. Like the SecurVantage Monitor, this unit also has two 10/100/1000 copper Ethernet ports, but it is optimized to handle traffic up to 200 megabits per second, or a full duplex fast Ethernet connection. This is ideal for monitoring perimeter connections. The Monitor LE is a combination of Harvester and Security Master in single unit. One Ethernet port gets connected to the span or monitoring location and the other is the management port that has the IP address.

E. SecurVantage Enterprise Manager

The SecurVantage Enterprise Manager (EM) allows centralized management of the SecurVantage Monitors installed in the enterprise. The Enterprise Manager can manage up to 25 monitors at one time, with identical or separate policies. Once a monitor is assigned to an Enterprise Manager, the monitor receives all policy updates from the Enterprise Manager. The Enterprise Manager collects the data from all of the Monitors assigned to it and presents an aggregate version of all of the results. The Enterprise Manager runs on a 1U rack mount server.

F. SecurVantage Enterprise Reporter

The Enterprise Reporter (ER) interfaces with the Enterprise Manager to generate reports based on the events collected by the SecurVantage product suite. The Enterprise Reporter can generate reports upon request, or can be configured to run specific reports on a periodic basis. The Enterprise Reporter runs on a 1U rack mount server.

G. SecurVantage Studio

SecurVantage Studio (SVS) is a Java based policy development and analyzer application. Studio requires a personal computer with an Intel Pentium III processor running at 500 Mhz or faster, with 512 MB RAM, 10 GB free space on the hard drive, a display set to 1024x768 pixels or greater and Windows 2000 operating system. It is used to develop the policies to be deployed onto the Monitors, and to examine the events that are flagged in violation of the policy. DME files can be downloaded from a Monitor and used to evaluate a new policy in development, or to verify that the changes made to an existing policy will function as expected. During the installation process, Studio will also install Sun Java2 Runtime Environment and Sybase SQL Anywhere on the workstation.

H. Security of the SecurVantage Product Suite

All hardware in the SecurVantage suite runs a hardened version of Linux, with no graphical user interface on the devices. Inbound communications are restricted to SSL and Monitors cannot initiate outbound communications. SSH is installed but disabled by default. The monitoring port on a SecurVantage monitor does not have a protocol stack implemented, and is not addressable or detectable.

During the installation, a self-signed digital certificate is generated on each piece of hardware. The digital certificate can be replaced with one issued specifically by your CA for this system after the installation is complete. Securify Monitors can be configured to trust and allow communications from one Enterprise Manager based on the digital certificates installed on both machines. The Monitors cannot initiate communications to the Enterprise Manager. The Enterprise Reporter must also be configured to communicate with the Enterprise Manager based on the digital certificates installed on both machines.

4. Information Gathering and Preparation

To successfully configure SecurVantage to audit the network perimeter, we need to have an understanding of the network being monitored.

- Addressing information for trusted internal subnets, including those subnets between the perimeter layers
- Addressing information for DMZ or untrusted subnets
- A list of ports and protocols allowed to traverse the perimeter
- IP addresses of important servers within the enterprise, especially servers that communicate across the security perimeter
- A detailed understanding of the Network topology

A. Information required to configure the monitor

In order to configure the hardware, there are several pieces of information required. The Management port on each monitor requires a viable IP address. If the equipment is going outside of the perimeter, addresses in the DMZ can be assigned. The perimeter routers can be configured to allow access to the Monitor addresses from the inside of the network, but not from the outside, as additional protection. Each system will need a DMZ IP address, the DMZ subnet mask and the DMZ default gateway. Each system will also need a fully qualified hostname, in the format *monitor.yourcompany.com*.

The system needs the correct time, adjusted to UTC, in a very specific format. This is important so that an accurate accounting of events can be made. If an Enterprise Manager is deployed to manage multiple Monitors, all of the systems need to be time synchronized. The format is MMDDhhmmYYYY, where MM is the two digit month, DD is the two digit day, HH is the two digit hour (in 24 hour notation), mm is the two digit minute and YYYY is the four digit year. So, January 7, 2004 at 2:45 PM would be 010714452004. During installation, use a nearby system to reference <http://tycho.usno.navy.mil/cgi-bin/timer.pl> for accurate UTC time.

The installation process will create a self-signed digital certificate for SSL and set the passwords for several system accounts. In a long term deployment, the self-signed certificate can be replaced with one issued specifically for this system. However, a certificate must be created during the installation process. To create the certificate, the installation program will need the 2 letter code for the country, the state or province, the city name, the company name, the system host name determined earlier, and an email address. Passwords will also be set for the admin, root, and svcs accounts. Be sure to document these passwords in a safe place, as these accounts will only be used when logging on at the monitor console, which is rarely done once installation is complete.

B. Example network information for this document

For the purposes of clarity during the rest of this document, a fictitious company will provide the details needed. Yourco consists of an “internal” network using the 172.16.0.0/16 network. Please see Figure 1 for the Yourco network diagram. Yourco has two connections to the internet with separate firewalls used by two different groups of departments. Their internal network is divided into several subnets for different departments and functions; however, the majority of the servers are in the 172.16.100.0/24 subnet. Each firewall consists of an inside router, a firewall, and an outside router, all connected via Fast Ethernet. The primary firewall has three interfaces installed, with interface one connecting to the outside router, interface two connecting to the inside router and interface three connecting to a switch that controls the DMZ. This may not seem like the best way to structure the perimeter, but this is just an example network to demonstrate perimeter monitoring.

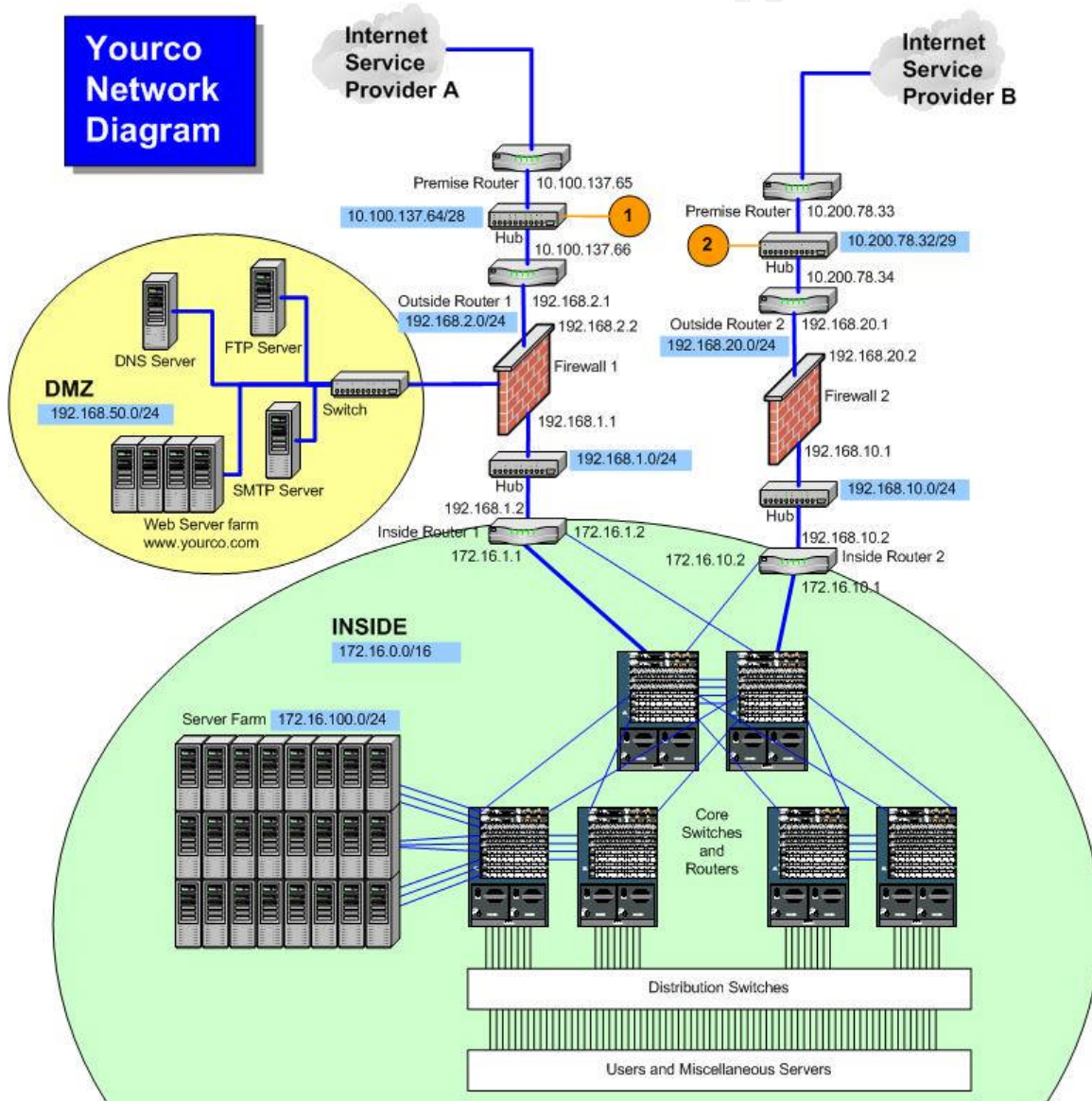


Figure 1 – Yourco Network Diagram

In order to monitor the traffic traversing the Yourco perimeters, two SecurVantage Monitors will be required. In Figure 1, these are represented by numbered orange circles. SecurVantage Monitors one and two will be installed between the outside router and premise router at each firewall. Since the perimeter is running Fast Ethernet, Monitor LE hardware will be sufficient, and no Enterprise equipment will be used. The management ports on the Monitors will be assigned addresses in the DMZ with 192.168.50.101 for Monitor Outside 1 and 192.168.50.102 for Monitor Outside 2.

C. Preparation

Prepare for the installation before the day of installation. If hubs will need to be inserted, coordinate that effort with the appropriate people. Plan for the work to be done after hours before the date of installation. Similarly, get the mirror ports configured, the IP addresses allocated, and any network configuration finished before the day of the install.

Identify which workstation will be used to run the SecurVantage Studio (SVS) and ensure that it meets the hardware requirements. Ensure that the most recent version of Internet Explorer is installed and functional. Install the SecurVantage Studio software before the day of installation and practice developing policies to become familiar with the interface.

© SANS Institute 2004, Author retains full rights.

5. Equipment Installation and Configuration

A. Hardware installation

Place the equipment in the location it will be used and connect the power and connect a keyboard and monitor to the first system. A monitor and keyboard will be needed to complete the installation, but these will not be required for normal operations.

B. Install the Monitor software

Boot the first Monitor LE from the SecurVantage installation CD and follow the steps presented on the screen. After the first phase is complete, the system will ask for the CD to be removed, and will then reboot. Once the CD has been removed from the first system, the installation will proceed without needing it. The install CD can be used to begin installation on the next Monitor while completing installation on the first Monitor.

During phase two of the installation, the UTC date/time will be required. After entering and verifying the date, the system will proceed to phase three and create and install database files. This will take about 40 minutes.

During this waiting time, the necessary cables can be run. Remember that one cable will need to run to a port for the monitoring connection and one cable will need to run to a port for the management connection for each monitor being installed. Remember to label the monitors "Outside1" and "Outside2" and label the cables appropriately.

After the system has finished creating the database files, the installation enters phase four. During this phase, the IP address information will be entered and the installation will create the self-signed digital certificate for SSL and several system accounts. Create the certificate by filling in the information requested. Then the passwords for the admin, root, and svs accounts will be requested. When all of these are entered, the system will reboot and the SecurVantage Monitor local software installation is finished.

The monitor and keyboard can be disconnected and the monitors are ready to connect to the network. Connect the management port of each SecurVantage monitor using the management cables you ran earlier. Then connect the monitoring ports using the monitor cables you ran earlier.



Figure 2 - Monitor LE Connections

C. Verify connectivity

Go to the SVS workstation and run Internet Explorer. Enter https:// 192.168.50.101 into the address box to connect to the management port in the Yourco example. If the following screen appears, the monitor has been successfully installed.

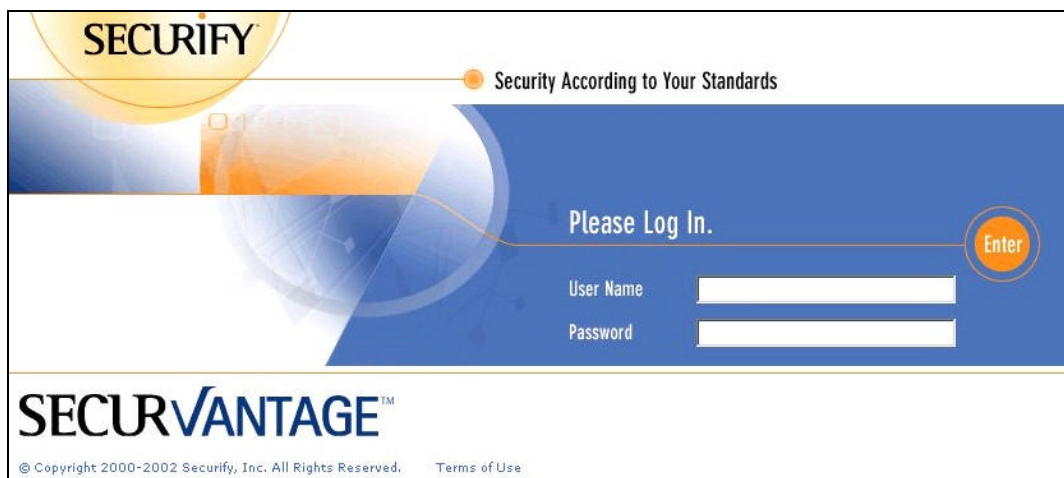


Figure 3 - Web Interface Login Page (Securify, p.8-22)

For future reference, bookmark the login screen. Log in as admin with the password entered during the installation process. A screen that looks like Figure 4, below, should appear. As this is a new install, the graph will be empty. Verify connectivity to each of the monitors that were installed.



Figure 4 - Web Interface Home Page (Securify, p.8-23)

D. Some Details on Policy Development.

The initial part of SecurVantage Studio policy development is similar to using a drawing program. However, a Securify “diagram” is not a detailed network diagram. It is a general outline of the network, only detailing the items important to the monitoring goals. Since the goal is to monitor the perimeter security, all subnets inside the perimeter can be distilled into as few subnets as possible. For example, Yourco owns a class B network (172.16.0.0/16) that is divided up to class C size sections for various departments (172.16.201.0/24 for sales, 172.16.202.0/24 for accounting, etc). In developing the Securify policy for perimeter security, the “inside” of the network would be drawn as one subnet with an address of 172.16.0.0/16. In a long term evaluation, the policy would be refined to identify additional details of the network, but even then it would not be necessary to draw additional boxes unless additional SecurVantage Monitors get deployed.

A Word on Criticalities

Securify reports events in six criticality levels: Critical, High, Medium, Warning, Monitor and OK. Part of policy development is determining which network events to report in each category to achieve the monitoring goals. Monitor and OK are both considered acceptable traffic and there is a difference in how SecurVantage handles them. Normally, SecurVantage records information about each network conversation, including the source and destination IP addresses, the source and destination ports, number of packets, and many other details. In the case of events found to match category OK, Securify records statistics. This keeps the internal databases down to a reasonable size and allows for more history to be stored. If it is deemed necessary to track the details of acceptable traffic for troubleshooting or other purposes, create a new outcome for the traffic that needs monitored, and change the Criticality in the new outcome to Monitor. Now set the outcome for the traffic to this new Monitor outcome in the Offering or Initiating rules. Just remember to change the outcome back to OK when the monitoring is completed, or the internal databases will not be able to collect as much history.

Defining Securify Rules

In a host or subnet detail dialog box, the Offering section governs the incoming traffic rules while the Initiating section covers outbound traffic. If the DMZ offers HTTP to the Internet with an outcome of OK, then any HTTP traffic from the Internet to the DMZ is flagged as OK. If the DMZ initiates HTTP traffic to the Inside with an outcome of Deny, then all of this traffic will show up as a violation in the SecurVantage Monitor. Rules are inherited from parent objects, and the default rules in a blank policy are to deny all ICMP, TCP and UDP traffic to all networks. In the default policy all traffic will be flagged as a violation. The optimal policy sets the rules at the correct level of detail to cover exactly the right number of hosts, in a similar fashion to Access Control Lists (ACL) in a router or firewall. For example, Yourco wants to allow FTP traffic inbound to the FTP server in the DMZ, but not inbound anywhere else. The easy way to define DMZ rules would be to identify the traffic at the DMZ subnet level, but this would allow FTP access to the other hosts in the subnet. The proper level of implementation would be to leave the DMZ subnet rules alone, and set the DMZ FTP Server to offer FTP with an outcome of OK. Since

the policy default is essentially “Deny All”, any FTP traffic to other DMZ hosts will be flagged as Deny. All Networks is a default entry for all of the defined networks, but use it as a source or destination with caution. As in a router ACL using “any any”, All Networks can have unintended results. Defining a rule to offer FTP to All Networks with an outcome of OK will result in FTP traffic from anywhere being classified as OK. This includes other DMZ hosts and traffic from the firewalls and routers. This may be what is intended, but be very sure.

Yourco wants to classify FTP traffic from the Internet or from the Inside to the DMZ FTP Server as OK, and deny all else. The rule would be defined on the DMZ FTP Host. To implement this rule, expand the hosts list in the left pane and double click on the DMZ FTP Server. In the first line under Offering, double click in the box under Service. Choose FTP from the drop down list. Double Click under To and choose the Internet. Double click again and choose Inside. The default outcome is OK for each destination. This brings out the point that allow and deny can be defined in the same rule. The Outside Firewall subnets could be added to this rule with an outcome of deny. However, the default Deny All will work in this case.

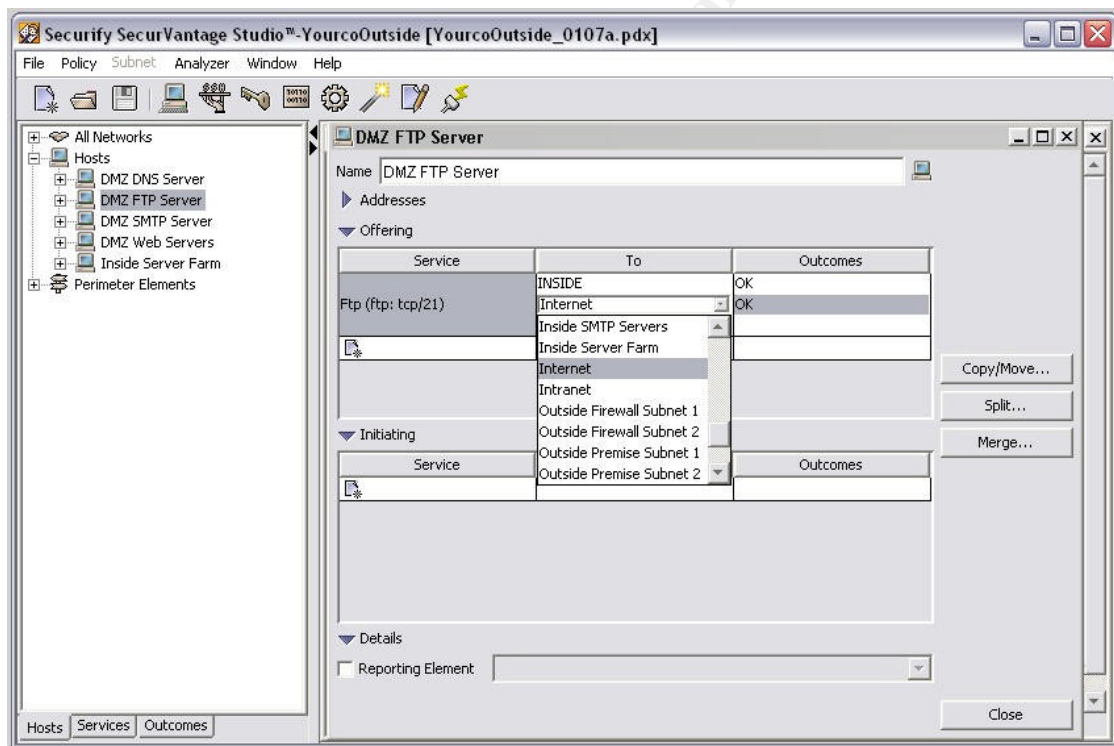


Figure 5 – Adding a Rule to a Host

Creating Custom Services and Outcomes

In the left pane of the main Studio window, there are three tabs at the bottom. Clicking on the Services tab brings it to the front, and we see that the default policy has defined many common services for us. Yourco decides to install a Microsoft SQL Server, which uses port 1433 by default, but port 1433 is not defined in the default policy. Clicking on the New Service Icon allows us to define this service for the policy. We will define the name as MS SQL Server, the base protocol as TCP Service and the target port as 1433. The Owner field allows us to enter point of contact information for the object. Clicking the close box adds the new service to our existing list.

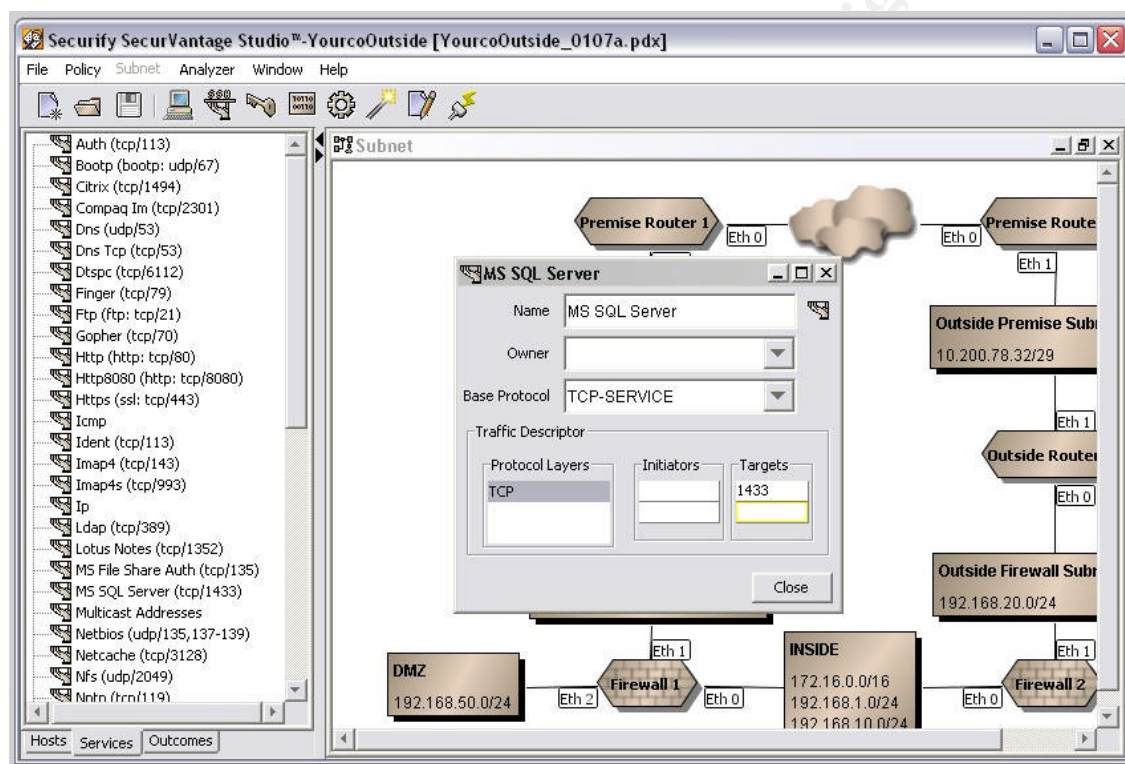


Figure 6 – Adding a Service

This brings us to the Outcome tab. The Outcome tab is where we define what Criticality level is associated with all aspects of an event. The basic protocols are defined in the base policy, but you can add your own outcomes or change the default outcomes. To examine an existing definition, double clicking on the OK under HTTP opens the Outcome Details dialog box. We can see that there are many components to HTTP traffic, and only three of them result in an OK criticality. Notice that if someone tries to use port 80 for something other than HTTP traffic, a High Critical event will be issued based on the component Non-HTTP Traffic. Double clicking on OK under TCP Service shows that TCP based outcomes will only have three components. In the Yourco policy, if MS SQL Server is given an OK outcome, a Connection Rejected event will cause a Monitor criticality, while Connection Accepted Data Transferred, or Connection Accepted No Data will return an OK criticality. Yourco is concerned about Connection Accepted No Data results for MS

SQL service and wants to monitor the traffic for signs of a virus attack. To monitor this traffic, a new outcome needs to be created under TCP Service. Right click on TCP Service and choose New Outcome. Change the name to MS SQL Monitor and change the Criticality for Connection Accepted No Data from OK to Warning and the Criticality for Connection Rejected from Monitor to Warning. This will elevate the criticality for these events, and make them more visible.

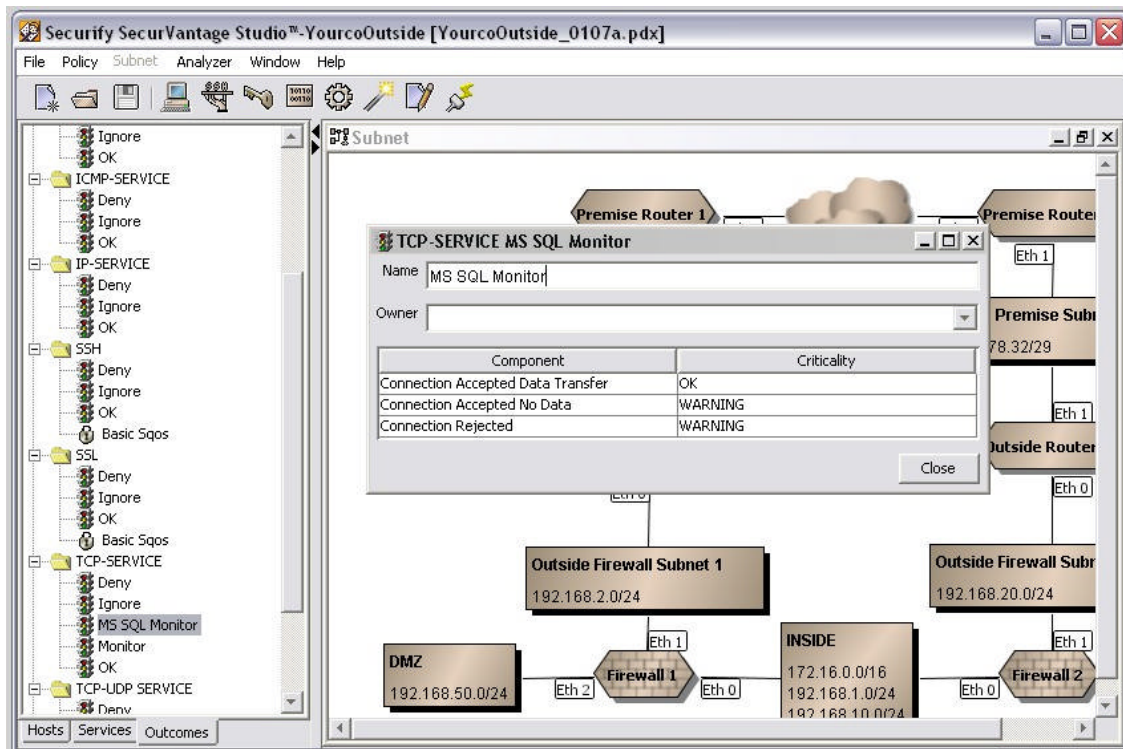


Figure 7 – Defining a New Outcome

Special Outcomes

Securify deals with some protocols in greater detail than most traffic. The details are explained in some of the Studio documentation. The most interesting aspect is the quality of service settings for SSL. SecurVantage refers to these settings as Security Quality of Service (SQOS) parameters. Studio allows extremely precise SSL parameter requirements, allowing different SQOS levels for different connections. For example, SSL connections from the Internet can be required to have client side certificates with a minimum key size of 2048 bits, use RSA Authentication and Key Exchange, have a minimum encryption strength of >96 bits(128 bit encryption) and use Triple DES encryption. At the same time, connections from the Inside can be configured with a more relaxed policy allowing various Authentication, Key Exchange and Encryption methods and 40 bit or higher encryption strength. Traffic that does not meet the minimum QOS settings can be classified as a High or Critical violation. The SQOS settings allow the security manager to keep tabs on the security of the web browsers leaving the inside of the network. SQOS settings can be defined for SSL communications to trading partners or trusted outside entities, like the accounting firm that is auditing your books.

Basic Sqos

Name: Basic Sqos

☐ Client Certificate Required

Minimum Client Key Size: 1024

Minimum Server Key Size: 1024

Protocol Versions: ☐ 2.0 ☒ 3.0 ☒ 3.1

Authentication

☒ Anonymous

☒ DSS

☒ Fortezza

☒ RSA

Key Exchange

☒ Diffie-Hellman

☒ Ephemeral Diffie-Hellman

☒ Fortezza

☒ RSA

Encryption

☒ 3DES

☐ DES

☒ Fortezza

☒ IDEA

☐ None

☐ RC2

☒ RC4

Minimum Encryption Strength

☐ 40 bits (Low)

☐ 56 bits (Medium)

☒ > 96 bits (High)

<input checked="" type="checkbox"/>	Cipher Suite	Authentication	Exchange	Encryption	Strength
<input type="checkbox"/>	SSL_RSA_WITH_NULL...	RSA	RSA	None	40 bits (Low)
<input type="checkbox"/>	SSL_RSA_WITH_NULL...	RSA	RSA	None	40 bits (Low)
<input type="checkbox"/>	SSL_RSA_EXPORT_WI...	RSA	RSA	RC4	40 bits (Low)
<input type="checkbox"/>	SSL_RSA_EXPORT_WI...	RSA	RSA	RC2	40 bits (Low)
<input type="checkbox"/>	SSL RSA EXPORT WI...	RSA	RSA	DES	40 bits (Low)

Close

Figure 8 – SQOS Settings

E. Policy development

Now, with the monitors in place and information about our topology, addressing schema, and allowed traffic in hand, we are ready to develop the initial policy.

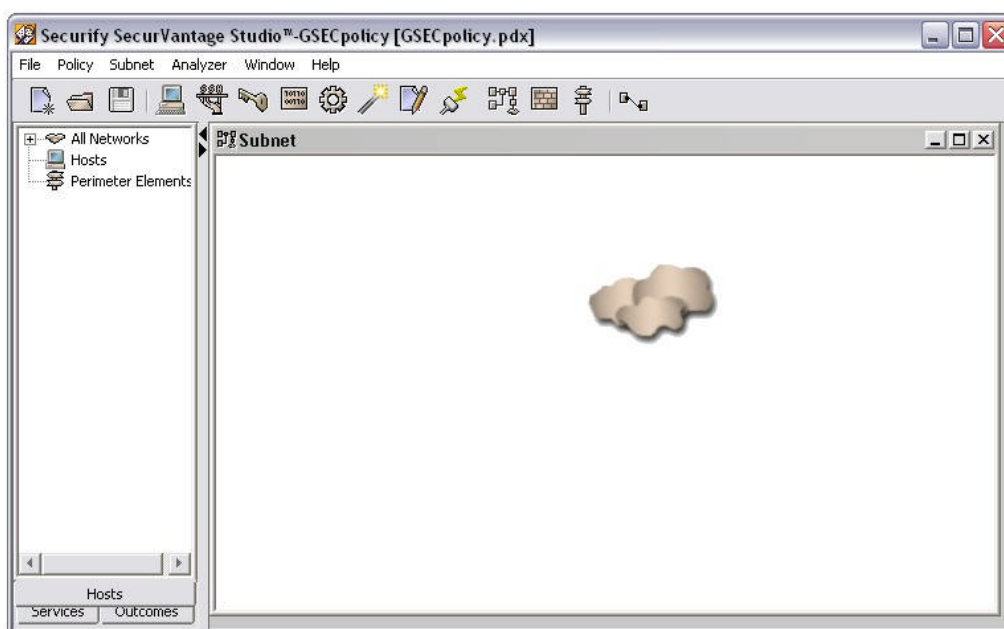


Figure 9 – Initial Blank Policy

Launch the SecurVantage Studio software and, under the File menu, pick New. First, name and save the file. Again under the File menu, pick Save As. This will open a dialog box asking for three pieces of information. For the Yourco example, type "YourcoOutside" in the Policy Name box. The policy name cannot have any spaces or underscores, and must start with a letter. Tab to the next box, File Name, and SVS will fill in the policy name followed by .pdx. I recommend appending a sequence number after the policy name to help keep track of revisions. For this example, I would change the file name from YourcoOutside.pdx to YourcoOutside_0107a.pdx. This indicates that this is the first (a) policy revision on January 7th. In the process of revise and deploy, after each deployment, choose save as and increment the letter. Click the button to the right of the third item, Working Directory, and navigate to the folder where the policy files will be saved. Click OK to save the Yourco policy file. Be sure to save your work often throughout the following steps.

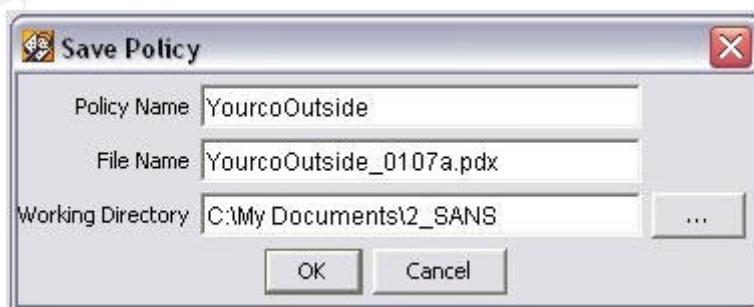


Figure 10 – Save Dialog Box

Under the Window menu, switch to the Subnet view. Now we'll begin to diagram our policy. The cloud at the top is a representative of the Internet. Any IP address not explicitly defined in the policy will be put in the Internet. Start by drawing the Inside subnet. Click the Insert Subnet icon and then click at the bottom of the subnet window. You will get a box labeled Subnet 1.

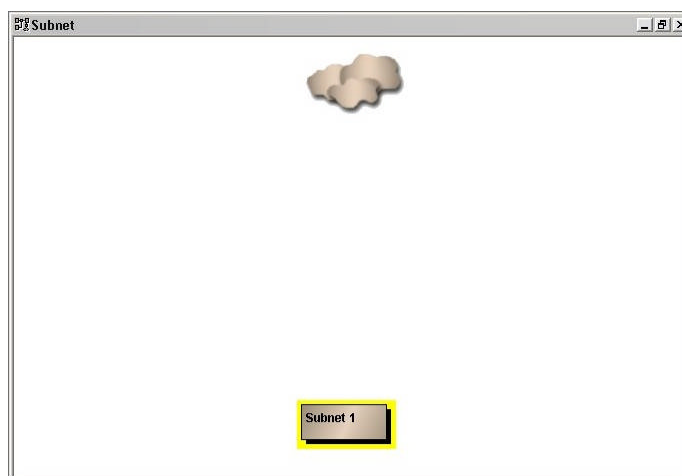


Figure 11 – First Subnet

Double click on this box and a dialog box will open, so that the details about this subnet can be filled in. For the example, change the name to Inside and click in the first address line. Entering addresses can be a little bit tricky. Enter the subnet address with CIDR notation, and be sure to tab out of the line before closing the dialog box. If you forget to tab out of the line, SVS will forget to save the line you just entered, resulting in a policy that does not work the way you expect. For the Yourco example, enter 172.16.0.0/16 in the first address line and hit tab. Enter the addresses for the subnets between the inside routers and the firewalls.

Figure 12 – First Subnet Detail Dialog Box

Remember, this drawing is a simplified logical diagram and not every piece of network equipment will be shown. Leave the Offering and Initialing sections empty for

now. The Subnet Type should be set to Intranet and the Collection Point and Reporting Element areas can be left alone for now. Click the Close button.

Now a firewall section can be laid out. Draw the Firewall 2 path first, as it is simpler. As you label the icons, stick to a labeling scheme to help identify direction flows during the analysis. Anything considered outside of the network gets “Outside” as the first word of its label. Anything in the DMZ will begin with DMZ and anything in the inside will get Inside at the beginning of its name.

SVS does not allow subnets to connect directly to each other, so a router or firewall has to be inserted. Click on the firewall icon and then click in the subnet window. Then add another subnet above the firewall. Notice that the name shows up as Subnet 1 again. This subnet box will be the subnet between Firewall 2 and Outside Router 2. Double click on the Fwall 1 icon that was just added and change the name to Firewall 2. The addresses of the firewall interfaces will be defined when the connectors get added. Double Click on the Subnet 1 icon and change the name to Outside Firewall Subnet 2. Add the IP address range of 192.168.20.0/24, tab and click Close.

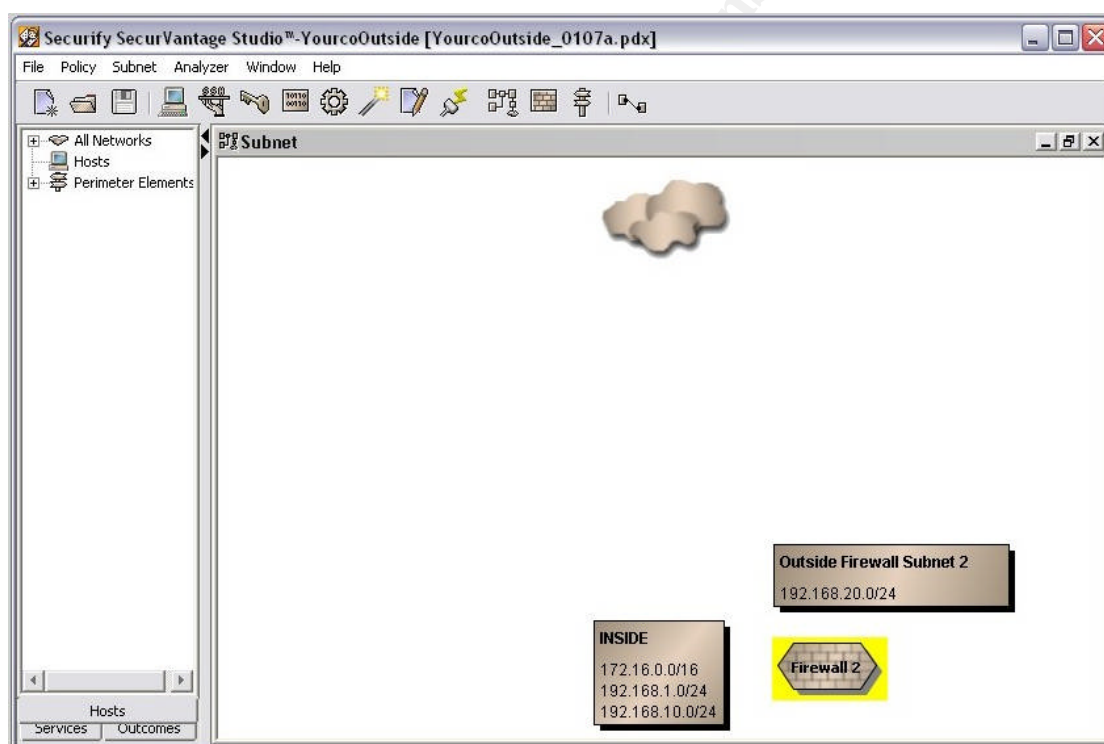


Figure 13 – Beginning Firewall 2 Path

Next, add Outside Router 2, the next subnet and the Premise router. Add a router to the picture and another subnet, and another router. Label the first router Outside Router 2, and label the second router Premise Router 2. Open the new subnet icon and change the name to Outside Premise Subnet 2 and add the address 10.200.78.32/29. This subnet will be where Monitor Outside 2 will gather traffic and this needs to be notated in the policy. Click the check box in front of Collection point, and SVS will fill in the Collection Point name, substituting underscores for spaces. Once this dialog box is closed, notice that the subnet box now has a magnifying glass icon, indicating the Collection Point is located here.

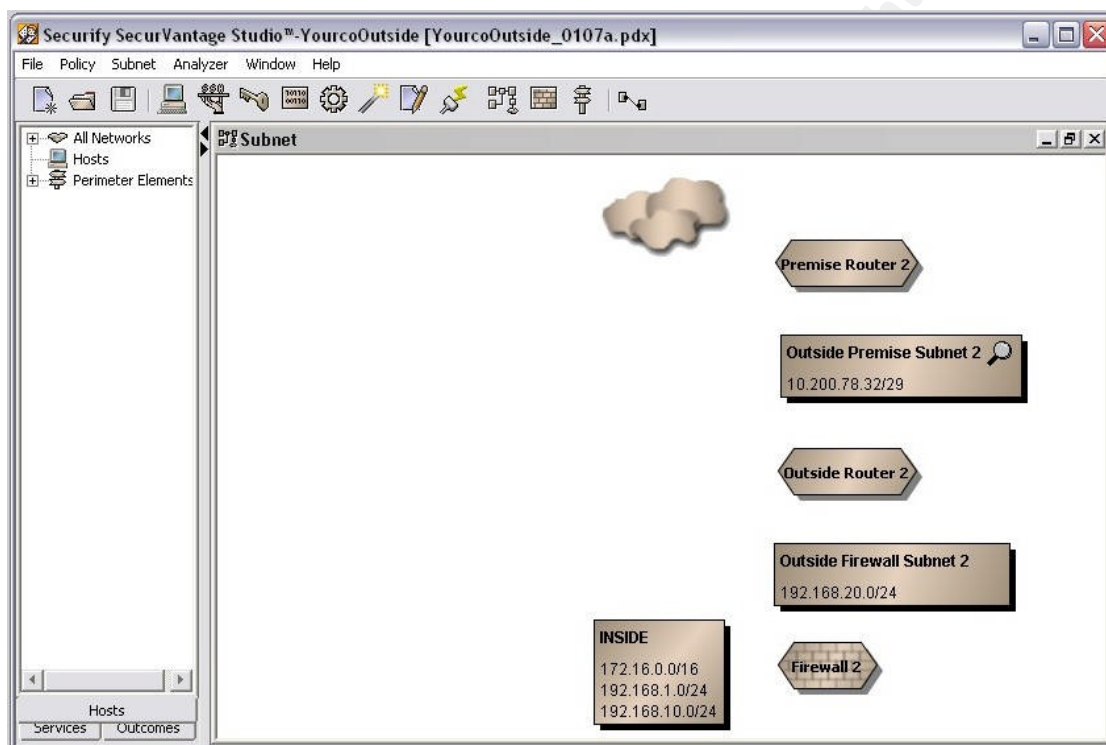


Figure 14 – Firewall 2 Objects

Now add connectors. Click on the connector icon and then click and hold on the Inside subnet. Drag to Firewall 2 and let go. A connecting line appears, labeled Eth 0. Double clicking the label will open a dialog box allowing the details of the connection to be filled in. The connection can be named to match the actual interface name on the real device. Add connectors between each of the icons, and add the IP addresses. We do not know the IP address of the connection from the Premise Router to the Internet, so leave that blank. If an incorrect address is entered, a warning dialog box will appear and SVS will make you fix it or remove it. For instance, SVS will not let you put 192.168.10.1 on either of the Outside Router 2 interfaces, because it knows that 192.168.10.0 is not in either of the subnets that the router is connected to.

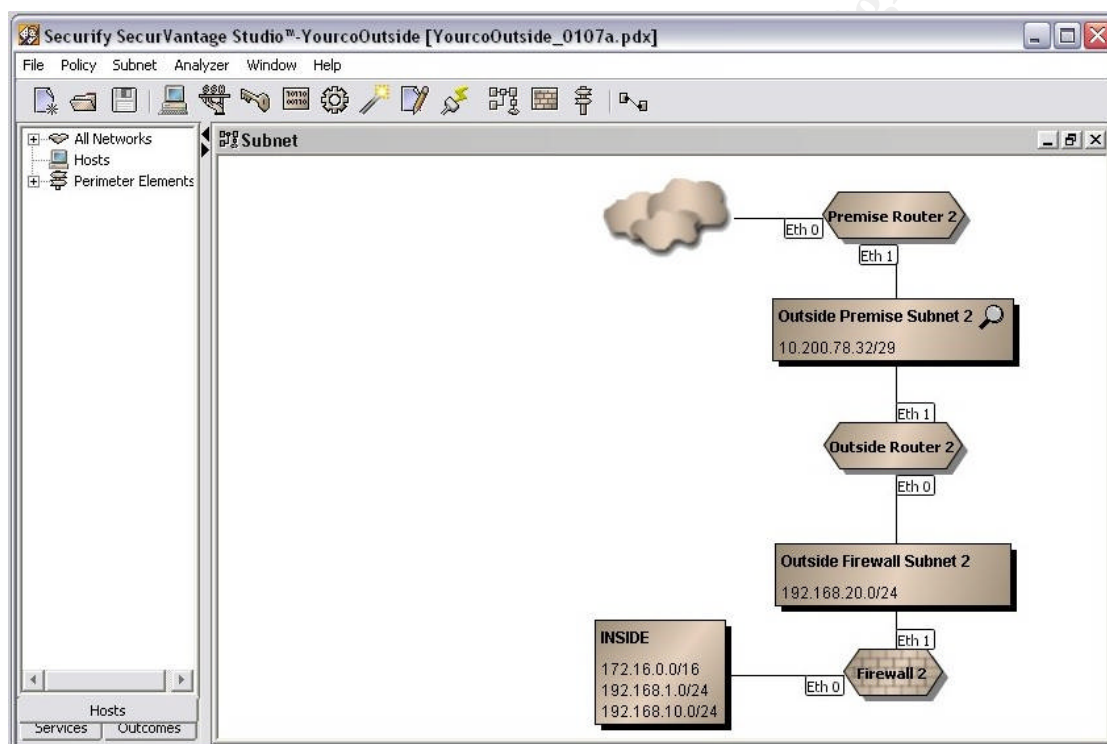


Figure 15 – Firewall 2 Path with Connectors

Now go back and add the Firewall 1 path as a duplicate of the Firewall 2 path. Don't worry about the DMZ, it will be added in the next step. Enter the correct addresses from the network diagram.

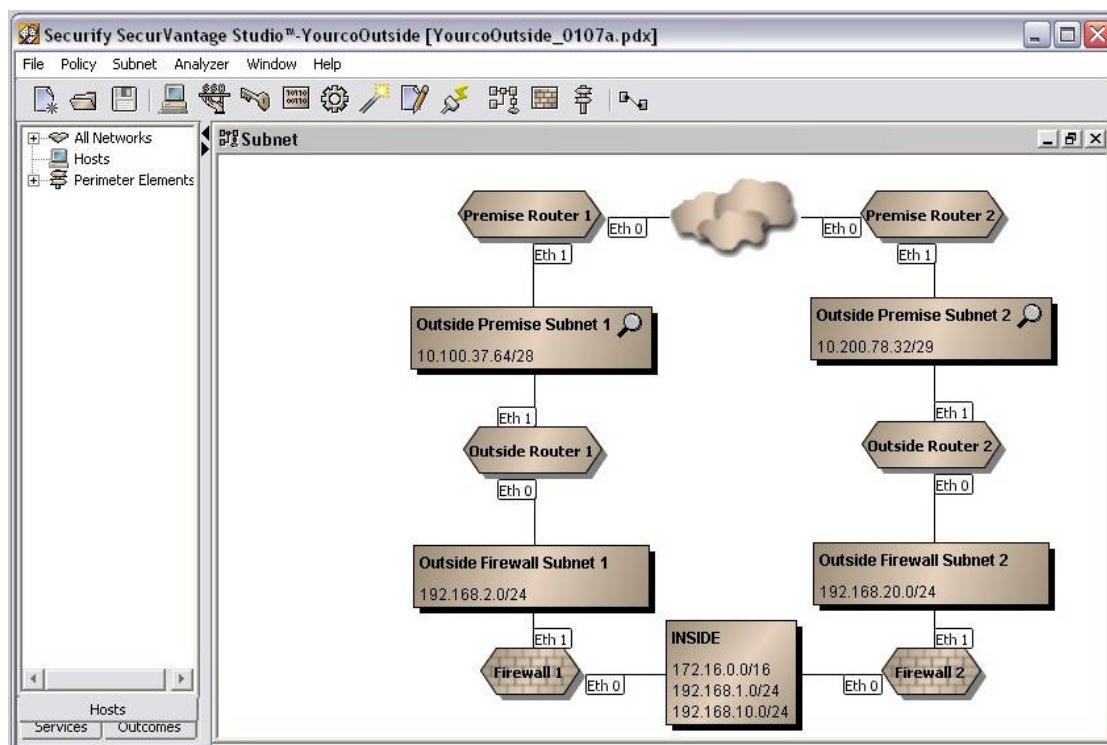


Figure 16 – Both Firewall Paths

Add another subnet to the left of Firewall 1. This will be the DMZ. Open the subnet and change the name to DMZ, but do not add an IP address. Close the dialog box and add a connector from Firewall one to the DMZ. In the left pane, click the plus symbols to expand the All Networks and Perimeter Elements items.

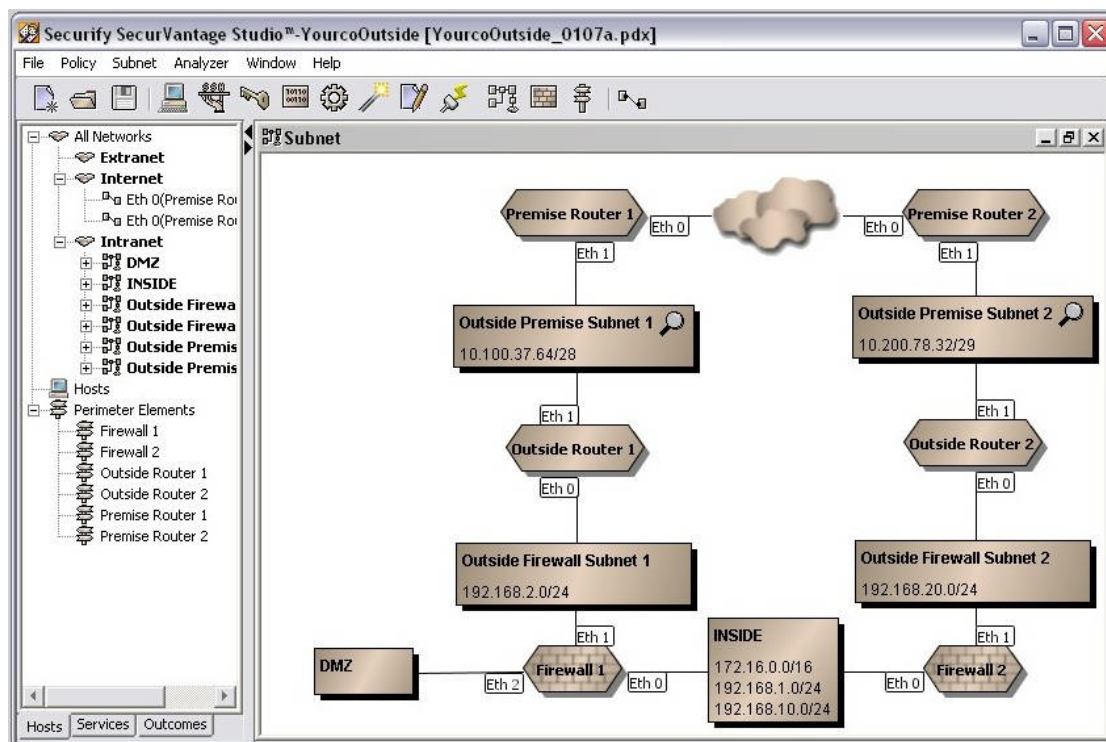


Figure 17 – Complete Policy Diagram

The “drawing” portion of the policy development is finished. Notice in Figure 17 that SVS has already determined which items are perimeter elements. The DMZ is grouped with the Intranet items because of its physical connection, since IP addressing has not been assigned. To illustrate a point, we’ll add the DMZ hosts before assigning an address to the subnet itself. Click the New Host icon and a dialog box will open. Change the name to DMZ DNS Server and enter the IP address 192.168.50.10 tab and click the close button. Add the DMZ SMTP Server at 50.11 and the DMZ FTP server at 50.12. Then add the DMZ Web Servers. Enter the address as 192.168.50.20-25 and press tab.

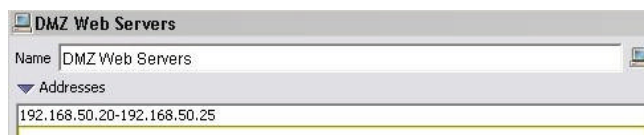


Figure 18 – DMZ Web Server Addressing

Notice in Figure 18 that SVS populates the address line as 192.168.50.20-192.168.50.25. Also notice in Figure 19, in the left pane, that while the DMZ hosts are all listed under the Hosts icon, they are also listed under the Internet icon at the top. Because a network address has not been entered for the DMZ subnet, SVS does not have a location to place these hosts. Anything SVS does not have a place for gets

assigned to the Internet. Close the host windows and add the address 192.168.50.0/24 to the DMZ subnet. As soon as the DMZ subnet detail dialog box is closed, the hosts jump to the DMZ subnet. See the right pane of Figure 19.

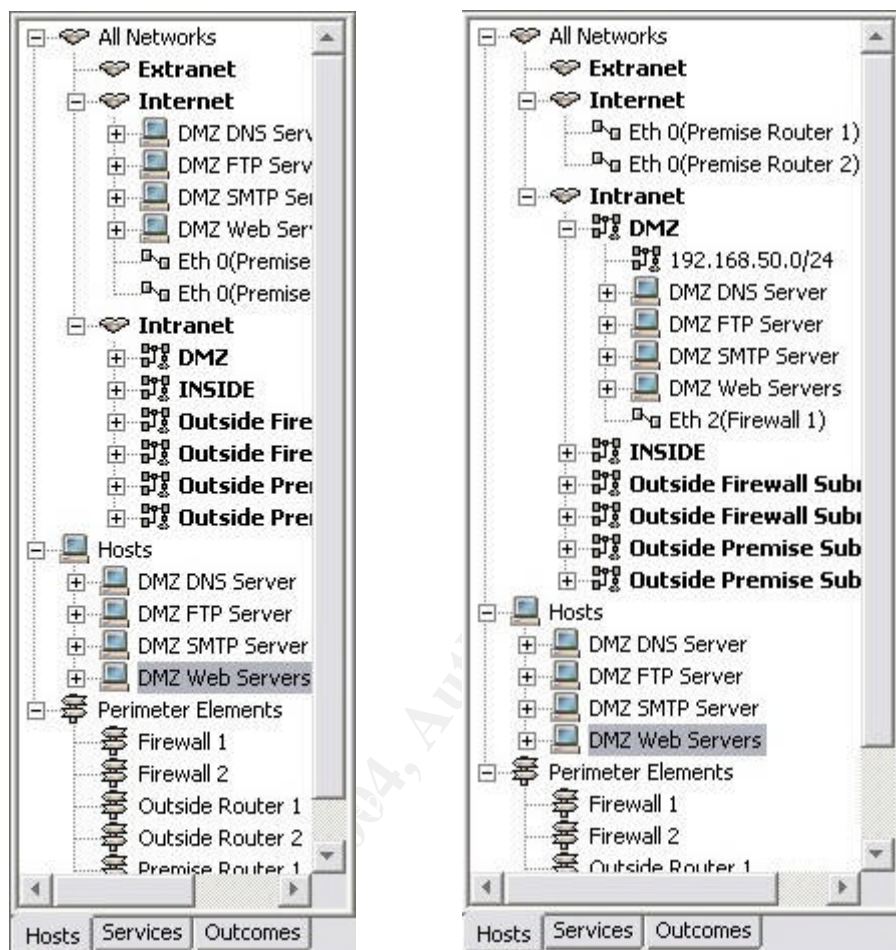


Figure 19 – Before and After Adding the DMZ Subnet Address

Now add another host and label this one Inside Server Farm. Give it the IP address range 172.16.100.0/24, tab and close. Add another host, and label it Inside DNS Server with the IP address 172.16.100.51. Add the Inside SMTP Servers at 172.16.100.65-69 and the Inside Intranet Servers at 172.16.100.100-109. Notice in Figure 20 that these Inside hosts get grouped under the Inside Server Farm host automatically.

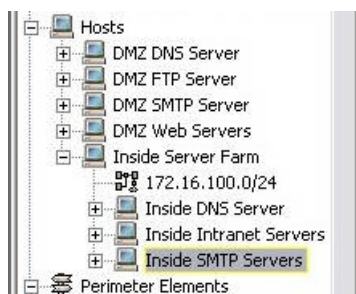


Figure 20 – Inside Hosts Grouped Automatically

Now that all of the parts of the network that are important to the policy have been laid out, rules can be defined to classify what is acceptable traffic and what is not. The rules are defined in the two sections passed over earlier - Offering and Initiating. We will add some simple rules allowing each server to offer and initiate traffic based on its function. Table 1 lists the initial rules for the Yourco network.

Object	Offer/Initiate Service	To	Outcome
DMZ DNS Server	Offer DNS	All Networks	OK
DMZ DNS Server	Initiate DNS	Internet	OK
DMZ FTP Server	Offer FTP	Inside Internet	OK
DMZ SMTP Server	Offer SMTP	DMZ Inside Internet	OK
DMZ SMTP Server	Initiate SMTP	Internet	OK
DMZ Web Servers	Offer HTTP	DMZ Inside Internet	OK
DMZ Web Servers	Offer HTTPS	DMZ Inside Internet	OK
DMZ Web Servers	Initiate SMTP	DMZ SMTP Server	OK
Inside DNS Server	Offer DNS	Inside	OK
Inside DNS Server	Initiate DNS	DMZ DNS Server	OK
Inside Intranet Servers	Offer HTTP	Inside	OK
Inside Intranet Servers	Offer HTTPS	Inside	OK
Inside Intranet Servers	Initiate SMTP	Inside SMTP Servers	OK
Inside SMTP Servers	Offer SMTP	Inside	OK
Inside SMTP Servers	Initiate SMTP	DMZ SMTP Server	OK

Table 1 – Initial Rules

Be sure to save after entering the rules. Also, notice that when a rule to Initiate is entered, the corresponding Offer rule is automatically defined. For example, after defining the rule to allow the Inside Web Servers to initiate SMTP to the Inside SMTP Servers, open the Inside SMTP Servers details. There will be a rule offering SMTP to the Inside Web Servers.

After these rules are entered, the policy is almost ready for initial deployment. Once a policy is modified, it needs to be run through the verification engine before deploying it. This process basically runs a consistency checker on the rules, making sure that they do not conflict. To verify the Yourco policy, under the Policy menu, choose Verify. A new window titled Messages will open, and scroll through a list of statements. There will be many statements like The “DNS” relationship offered by “DMZ DNS Server” to

“All Networks” PARTIALLY overrides the “UDP” relationship offered by “All Networks” to “All Networks”. This is letting you know that the policy defined for DMZ DNS Server will modify the response of the all networks policy, which is the intended result. However, the statement The “Smtp” relationship offered by “Inside SMTP Servers” to “Inside Intranet Servers” REDUNDANTLY overrides the “Smtp” relationship offered by “Inside SMTP Servers” to “INSIDE” indicates a rule that can be removed. The “Inside SMTP Servers” to “Inside Intranet Servers” rule will generate the same result as the “Inside SMTP Servers” to “INSIDE” rule, and in the interest of simplification, should be removed. Leaving the rule in the policy will cause additional work for the Monitors, and in a large policy many redundant statements could slow the system down. In this simple policy, it will not cause any problems to leave it in place. If there are any errors in the message window, they must be corrected before deploying the policy.

This is an initial policy and will require refinement. For example, any traffic originating “Inside” and headed for the Internet will be flagged as a violation. Also, the traffic to the management ports of the Monitors will be classified as a violation – HTTPS is only allowed from the inside to the DMZ Web Servers. After the policy is installed, the initial refinement process will classify the majority of the traffic into one of the outcomes.

© SANS Institute 2004, Author retains full rights.

F. Policy installation

In the Yourco example, two Monitors are being installed without an Enterprise Manager. If Yourco had deployed an EM, the policy would be uploaded to it, and the EM will distribute the policy to the Monitors. Since Yourco does not have an Enterprise Manager, the policy will need to be tweaked for each monitor and then uploaded to each Monitor individually. First, modify the policy for Monitor Outside 1, in Outside Premise Subnet 1. Double click on Outside Premise Subnet 2 and turn off the Collection Point checkbox. Save the policy and verify it again. Close the policy file in Studio by choosing New under the File menu.

Connect to Monitor Outside 1 with Internet Explorer and log in with the administrator credentials. On the home page, click the Manage tab. On the main Manage screen, click the word Configure Systems on the blue bar under the Manage tab. The left pane of the window will have the policy domain name, with the monitor listed under it. Click on the policy domain name. In the main window, the General Configuration tab will be displayed, with the default information filled in. Change the policy name to the name used when the file was initially saved, YourcoOutside, and click the Browse button. Locate the policy file, YourcoOutside_0107a.pdx, and click OK. Verify that the time zone is set to match the local time zone. Click the Submit Changes To Configuration button to upload the new policy and save the settings. Click the Live Data button at the top to return to the home page. After about five minutes, the graph will start to populate with the results of the new policy.

Now tweak the policy for Monitor Outside 2. Open the policy in Studio, double click on Outside Premise Subnet 2 and turn on the Collection Point checkbox. Double click on Outside Premise Subnet 1 and turn off the Collection Point checkbox. Save the policy and verify it again. Close the policy file in Studio by choosing New under the File menu.

Connect to Monitor Outside 2 and log in. Repeat the same steps for Monitor 2 as you did for Monitor 1. At this point, both monitors should have a good policy and should be monitoring traffic.

© SANS Institute

G. Policy refinement

After the monitors have had the policy installed for a few hours and monitored a sufficient amount of traffic, Policy refinement can begin. There is a way to have the Monitors generate DME files that can be downloaded to the SecurVantage Studio workstation for offline analysis and policy generation. We will look at how to connect SVS to the Monitors to use online analysis in policy refinement.

Open SecurVantage Studio and open the latest version of the policy. Under the Analyzer menu choose View Connections. This will open a dialog box where connection information can be added or edited. Both of the Yourco monitors need to be added to this list. Double click in the first empty box under Name and enter Outside 1. Double click in IP address and enter 192.168.50.101. If the hostname assigned the monitor is entered in the corporate DNS, SVS will populate the DNS name box. Repeat for Outside 2.

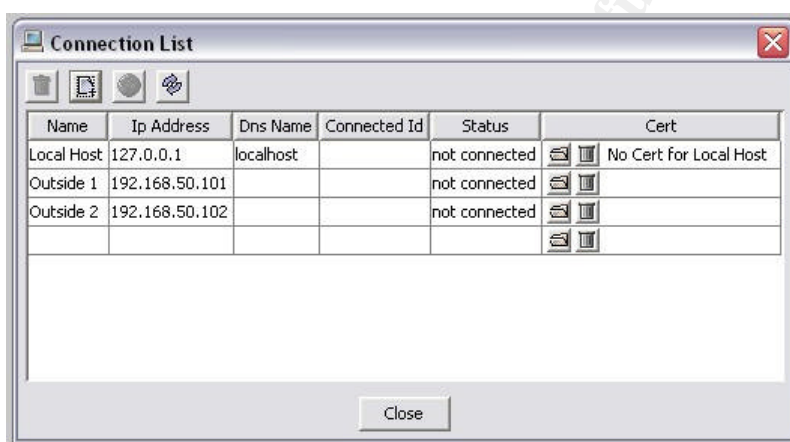


Figure 21 – Connection List Dialog Box

Now close the Connection list box and choose Connection under the Analyzer menu. Use the pull down Name field to choose Outside 1, and enter the administrator credentials. Click the None radio button under Query and then click OK.

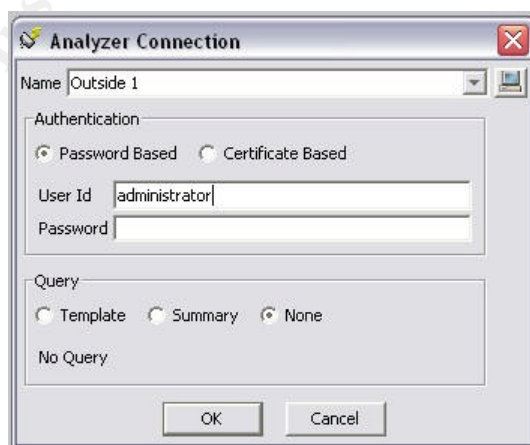


Figure 22 – Analyzer Connection Dialog Box

A new window will open labeled Workbook.

(NOTE: As Yourco does not exist, the next several images will not be showing a live connection but a local host connection. The procedures are the same, but in a live connection, you would be able to choose the time interval in the upper left area of the window, instead of choosing a file.)

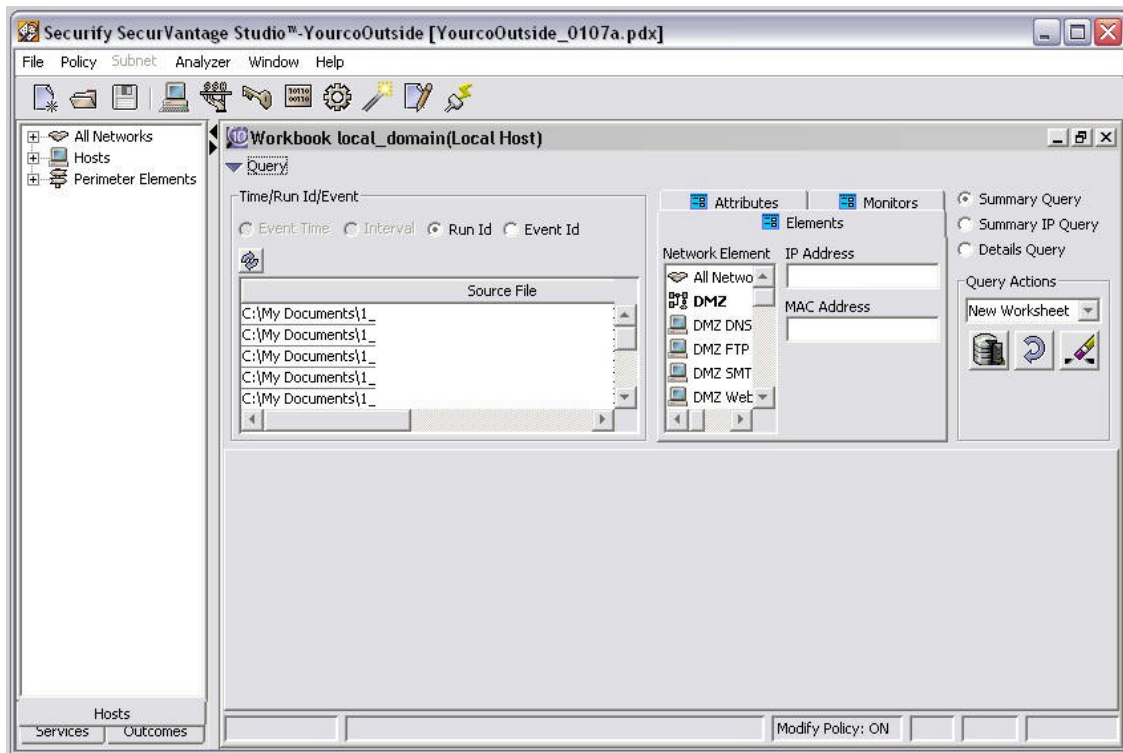


Figure 23 – Initial Analyzer Workbook

In the center of the window are three tabs that allow queries to be filtered: Elements, Attributes and Monitor. On the right side, the radio buttons allow you to choose the type of query and the three buttons perform the functions in Table 2.




	Perform Query
	Reset Query Parameters
	Clear Query Parameters

Table 2 – Analyzer Buttons

For the initial policy refinement query, accept the default time interval (which is the previous 24 hours), apply no filters and click the Perform Query button. This generates a table in the lower half of the window.

#	Source Network Element	Destination Network Element	Service Protocol	Service	Count	Criticality	Outcome	Outcome
1	Internet	INSIDE	TCP	Http	3	HIGH	Builtin	Invalid
2	Internet	INSIDE	TCP	Https	1305	HIGH	Builtin	Invalid
3	Internet	INSIDE	UDP	Snmp	16	HIGH	Builtin	Invalid
4	Internet	INSIDE	UDP	Udp	1	HIGH	Builtin	Invalid
5	Internet	Internet	ICMP	Icmp	15	HIGH	Builtin	Invalid
6	Internet	Internet	IP	Ip	18	HIGH	Builtin	Invalid
7	Internet	Internet	TCP	Ftp	1	HIGH	Builtin	Invalid
8	Internet	Internet	TCP	Http	174	HIGH	Builtin	Invalid

Figure 24 – Initial Analyzer Workbook

The entries in the table are summaries of the events that Securify monitored. They appear in the table grouped by Source Network Element, Destination Network Element, Service Protocol and Destination Port, if the port is defined in the policy. So, all TCP Port 25 conversations from the DMZ SMTP Servers to the Internet (outbound) will be summarized on one line. TCP Port 25 conversations from the Internet to the DMZ SMTP Servers (Inbound) will be summarized in a second line. However, TCP traffic from the Internet to the Inside that does not have a service definition will all get summarized on one line. The count column indicates the number of conversations summarized. Double clicking on the summary line will open a detail tab with one line for each conversation monitored, and includes the source and destination IP addresses.

Clicking on a column heading will sort by that column, holding the shift key down while clicking on a second header will do a secondary sort. For example, click once on the Criticality header to sort the events with the High violations at the top. Hold the shift key down and click twice on the Count header to put the highest count High violations at the top.

Count	Criticality
2032	HIGH
1305	HIGH
306	HIGH
183	HIGH
174	HIGH
137	HIGH
96	HIGH
61	HIGH

Figure 25 – Sort by Criticality and Count

Before the policy can be refined, it needs to be determined if it is a correct mapping of the network. If the outcome of an event in this summary query is “Invalid Route”, the policy definition is saying that the Monitor should not be seeing the traffic. For example, the Yourco routers are placed outside the outside router. Any traffic between the DMZ and the Inside network should never be seen by the Monitors, as well as traffic with Internet as both the Source and Destination. This means that there is a flaw in the network “drawing” in Securify. If the monitor is seeing traffic that should be “inside” of the monitoring points, there are several possible reasons. There could be a typo in the policy. Misconfigured network equipment could be directing the traffic to the wrong destination. Or, someone could be spoofing the network addresses in an attempt to penetrate the perimeter security. If Internet to Internet traffic is visible, there are probably addresses inside the network that are not defined in the policy. Perhaps someone has plugged a wireless access point into the network drop at their desk, and is passing out addresses to wireless users. Investigate where this traffic is coming from and either fix the policy or fix the network. According to the NSA Router Security Configuration Guide:

Reject all traffic from the internal networks that bears a source IP address which does not belong to the internal networks. (Legitimate traffic generated by sources on the internal networks will always bear a source address within the range or ranges assigned to the internal networks; any other traffic is attempting to claim a bogus source address, and is almost certainly erroneous or malicious in nature.)

Reject all traffic from the external networks that bears a source address belonging to the internal networks. (Assuming that addresses are assigned correctly, traffic sent from the external networks should always bear a source address from some range other than those assigned to the internal networks. Traffic bearing such spoofed addresses is often part of an attack, and should be dropped by a border router.)

Reject all traffic with a source or destination address belonging to any reserved, unroutable, or illegal address range. (Antoine, p.39)

This advice is sound for policy development as well as router configuration. A list of the special use IP addresses is available in RFC 3330 from the Internet Assigned Numbers Authority. (IANA, RFC 3330) This list was consulted to develop the IP address structure used in the Yourco example network. Additionally, SANS publishes a list of common vulnerable ports and an index of the top vulnerabilities in both UNIX and Windows systems (SANS). It is advised to review these vulnerabilities and take them into account when refining your policy.

If the policy changes to reflect new findings about the network, be sure to run the verification and save the updated policy with a new sequence number. Allow the updated policy to run on the monitors for a few hours and then run a new summary query.

Once the Invalid route entries are taken care of, proceed to refine the policy. Sort the query so the highest count High violations are at the top. Double click on the first violation to generate a detail report. Examine the detailed results and determine if the traffic should be acceptable according to your monitoring criteria. For the Yourco example, HTTP traffic from the Inside to the Internet should be OK. Since Yourco wants to allow this for all Inside to Internet traffic, go back to the summary tab and right click on the number to the left of the summary line. From the pop up menu, choose Create Policy. In the dialog box, confirm the details, including the outcome, and click Accept.

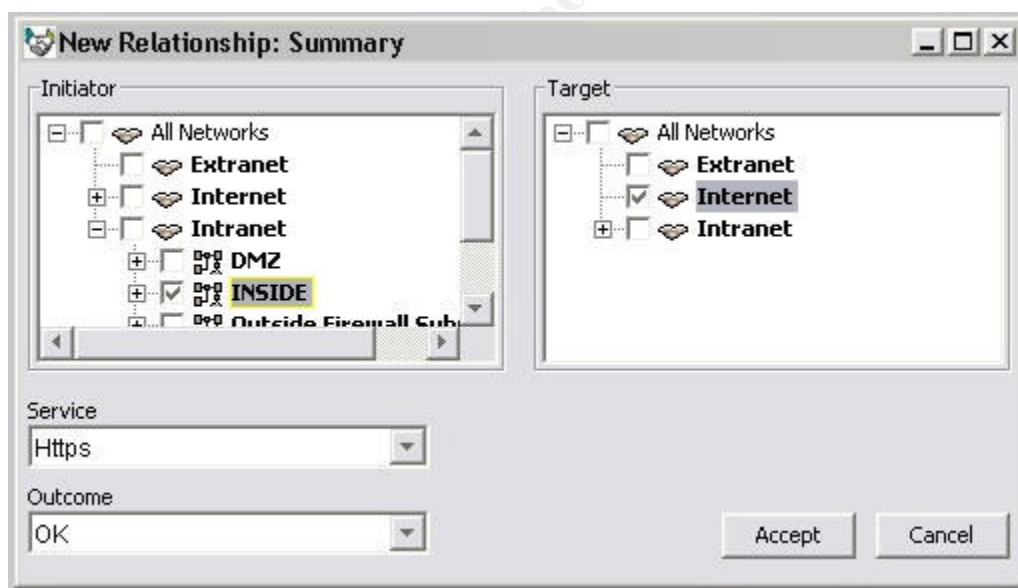


Figure 26 – Refine Policy in Workbook

This will add the new rule to the policy. Back in the workbook window, right click on the number again, and choose “remove row #”. This will delete the row from the summary list since it has been dealt with. This does not delete the data from the database, just from the display being examined. Remove the detail tab in the same manner - right click on the detail tab and choose Remove. Repeat this process of examine details, add to policy (or not), and remove the rows, until all of the summary lines have been evaluated. Now, re-verify the updated policy and save it with a new

sequence number. This process can be repeated until a good baseline of the network traffic has been established.

An additional method to assist in identifying traffic is to create host groups in the Internet. Create one group of "BAD HOSTS." Systems that have caused large amounts of violations, such as a system that has performed a port scan on your network, will get added to this group. Set the outcomes so that anything coming from or going to this group gets flagged as a High or Critical violation. Create a second group of "Trusted Hosts." Place systems in this that belong to companies or organizations that you trust, but are outside your security perimeter. Trading partners or subsidiaries on the other end of a VPN connection are good candidates for inclusion in this group.

© SANS Institute 2004, Author retains full rights

6. SecurVantage Monitor Web Interface

Traffic can be monitored via the Web interface. Logging in to the Monitor will display the home page. This page contains three graphs, a chart of the violations, and a table showing a breakdown of the number of events falling into each Criticality for each subnet defined in your policy. The first graph and chart are color coded, indicating the severity of the violations.



Figure 27 – Web Interface Home Page (Securify, p.8-23)

The analyze tab allows you to see information similar to a summary query in the Web GUI. Clicking on the headers will sort the data by that column. Sliding the handles on the bar at the bottom of the screen will adjust the time interval for the query. The default is the past 24 hours, and it can be adjusted to as short as one hour or as long as the past two days. Click on a Reporting Element name to see a summary query for the traffic originating in that element. If the traffic is any criticality other than OK, the word view appears next to the Source Element name. Clicking on view is the similar of the detail tab in Studio. The Web Interface will display the source and destination IP addresses, the service, the port and the count of conversations. This section of the Web Interface can be used to perform some initial analysis of the events, but for detailed analysis SecurVantage Studio is the correct tool.

7. Evaluating results

A. General

If the policy is an accurate depiction of the traffic allowed to traverse the perimeter, the Violation graph should be small. It is only depicting violations and monitor traffic. The graph on the top right is showing the total events monitored by this system. In a business that works a 9 to 5 type schedule, this graph usually will display a plateau shape. Overnight, the graph should be flat and low, indicating little or no traffic. When the early birds start to arrive, the traffic will slope upward, flattening off around 9 a.m., when the bulk of the users are arriving, logging in, and checking email. The graph will stay fairly consistent, usually showing a rise near 5 p.m., when users finish up for the day. This small peak is followed by a downward slope as the users log out and head home, tapering off through the evening as those working late sign off and go home. Usually by 8 or 9 p.m., the graph should be fairly low, and stay that way throughout the night. See figure 27 for a graph similar to the one described.

If the graph deviates from the general shape described, or the normal shape for your network, the discrepancy should be investigated. If an intruder were to perform a port scan on an address in your network you will see a large vertical line where the port scanner probed a large number of ports in a short time, causing the traffic load to exceed the normal levels by 100% or more. According to Lee, Roedel and Silenok from the Department of Computer Science & Engineering at the University of California, port scans usually fall into one of three categories:

- Horizontal port scans are attacks where an intruder chooses a port and scans that one port on many systems in your address range.
- Vertical attacks are where the intruder chooses a single system and scans many port on that single host.
- Block Scans are combinations of horizontal and vertical scans. (Lee, et al, p.2)

One of the most common port scanners is nmap, a freeware tool available from www.insecure.org. The default setting for nmap is to scan ports 1 to 1024 on the target in a fairly short amount of time. Nmap can use a subnet as a target by simply entering an asterisk instead of the last octet or two of the target address, resulting in a block scan. (Fyodor, www.insecure.org)

B. Summary IP Query

Another evaluation tool is the Summary IP Query. This query generates a more detailed result than the Summary Query. In this query, each line indicates a Source IP address-Destination IP Address-Destination Port summary. Sorting this by Source IP provides an interesting picture of who is originating traffic, while sorting by Destination IP provides a look at who are the big recipients on the network. Sorting by Source IP and then Destination Port can reveal Horizontal port scans of the network. Right clicking on an item, like an IP address or a port number, brings up a menu that allows filtering, as well as policy modification. Right click on the destination port number in a line displaying Port 53 traffic and choose Only '53'. SVS will hide all lines that do not have DNS traffic. Right click again and choose Unhide to display the other lines.

C. Getting data out of Securify

There are many ways to query and sort in SecurVantage Studio. However, if the options in the Studio do not provide sufficient analysis options, the data can be moved into other programs for additional analysis. As long as the line count in the lower left corner of the workbook window does not exceed the row limit in Excel, it is easy to copy and paste a query result. Right click on the tab for the window you wish to copy, choose Copy to Clipboard, click in cell A1 of an empty Excel file and click Paste. This is also a good way to archive data for forensic analysis. Yourco begins to see a spike around 1 a.m. every night. The Security Manager queries the Monitors to determine the source of the anomalies, refining the query to show just the anomalous traffic. Each query result gets copied and pasted into a new worksheet in an Excel file so that they can be archived and compared. This operation becomes even easier with Enterprise equipment deployed. An Enterprise Manager allows queries across multiple monitors. An Enterprise Reporter can produce more complex reports that include summaries and totals. ER reports can be saved in several formats to your local workstation.

8. Summary

This document has been a basic tutorial on installing Securify products for the first time. I have shown how to install the hardware, develop an initial policy and perform initial policy refinement. In several cases, information learned in just performing these steps has allowed large enterprises to close security holes that they were not even aware of. This is a stepping off point, and as you become more proficient with Securify as a tool in your security toolbox, the more ways you will find to use it.

© SANS Institute 2004. All rights reserved. Author retains full rights.

9. References

Scott, Steven. "Threat Management Systems, The State of Intrusion Detection." August 9, 2002. URL: <http://www.snort.org/docs/threatmanagement.pdf>

"Securify Introduces First Automated Network Security Management System; Securify SecurVantage(TM) Boosts Protection, Simplifies Network Operations, Reduces Costs." PR Newswire. July 15, 2002. URL: http://www.findarticles.com/cf_dls/m4PRN/2002_July_15/88988749/p1/article.jhtml

Securify. "Company Information." URL: <http://www.securify.com/company/>

ITsecurity.com. "Securify Scales SecurVantage to the Next Level." June 4, 2003. URL: <http://www.itsecurity.com/tecsnews/jun2003/jun28.htm>

Sturdevant, Cameron. "Securify Nabs Intruders." eWeek. January 20, 2003. URL: <http://www.eweek.com/article2/0,4149,838310,00.asp>

Antoine, Vanessa, et al. "Router Security Configuration Guide." National Security Agency Report Number C4-040R-02 version 1.1. September 27, 2002. URL: <http://nsa2.www.conxion.com/cisco/guides/cis-2.pdf>

IANA. "Special-Use IPv4 Addresses." RFC 3330. September 2002. URL: <http://www.rfc-editor.org/rfc/rfc3330.txt>

SANS. "The Twenty Most Critical Internet Security Vulnerabilities (Updated) ~ The Experts Consensus." Version 4.0. October 8, 2003. URL: <http://www.sans.org/top20>

Lee, Roedel and Silenok. "Detection and Characterization of Port Scan Attacks." Department of Computer Science & Engineering, University of California, San Diego. Winter 2003. URL: <http://www.cse.ucsd.edu/users/clbailey/PortScans.pdf>

Fyodor. Nmap documentation. URL: http://www.insecure.org/nmap/nmap_documentation.html

Graphics on page 10 and page 33 are from:

Securify. "Securify SecurVantage Version 3.1 Training Guide." Electronic documentation provided by Securify. 2002.

Remaining graphics are screenshots from actual SecurVantage Studio.

References that contributed to the writing of this document

Securify. "Securify SecurVantage Version 3.1 Installation Guide." Electronic documentation provided with SecurVantage Studio. November 2002.

Securify. "Securify SecurVantage Version 3.1 Operations Guide." Electronic documentation provided with SecurVantage Studio. November 2002.