Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Configuring a NetScreen Firewall: Best practice guideline for the basic setup of a NetScreen firewal

Firewalls are generally accepted as the best defense for network security. This paper will detail how to setup a NetScreen firewall using the command line configuration options. It will demonstrate how to setup the trusted and untrusted ports, management IP address, SNMP, DNS and some critical security policies. The report will also show how to configure the syslog reporting, administrator email alerts, and the DHCP server. NetScreen firewalls use an operating system called ScreenOS, an original OS created for firewall...

Copyright SANS Institute
Author Retains Full Rights

AD
observe it
MANAGE THE RISK OF YOUR USERS
FREE USER
ACTIVITY MONITORING
TRY IT NOW

Configuring a NetScreen Firewall

Best practice guideline for the basic setup of a NetScreen firewall using the command line configuration options

The Practical Assignment for the SANS GIAC Security Essentials certification

Assignment version 1.3

April 2002

By
Robert Bayley

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Table of Contents

Introduction……..……..……..……1
Basic Defense in Depth……..……..……..……1
Command Line Tips...……..……1
Firewall Operation Modes……..……..2
Getting Started……..……..……..…3
Setup on the Network……..……....……...4
Good Security Practices……...……..……..……6
Creating a VPN Tunnel……..……..…9
Summary….……..…..……...…11
Appendix A……..……...…12
Appendix B……..……...…18
Sources…….……..……19

© SANS Institute 2002, Author retains full rights.

Introduction

Firewalls are generally accepted as the best defense for network security. This paper will detail how to setup a NetScreen firewall using the command line configuration options. It will demonstrate how to setup the trusted and untrusted ports, management IP address, SNMP, DNS and some critical security policies. The report will also show how to configure the syslog reporting, administrator email alerts, and the DHCP server.

NetScreen firewalls use an operating system called ScreenOS, an original OS created for firewalls and virtual private networks that runs on a custom designed ASIC. Although there is a web GUI interface available to configure most options, this paper will detail the basic command line configuration as well as suggestions to improve firewall security by limiting logins, configuring a firewall management station and improving egress filtering and logging. In the final section of the paper, the report details how to configure a LAN-to-LAN IKE VPN tunnel using 3DES encryption and SHA-1 authentication.

For the purposes of this paper, we will be using a NetScreen 5XP in network address translation mode with ScreenOS version 3.01. These basic command line settings remain the same for other NetScreen products and can be applied to corporate enterprises and home offices.

Basic Defense in Depth

A firewall is critical to establishing good network security and is a vital first component of network defense in depth. Dorothy Denning in *Information Warfare and Security* states, "Defense in depth is the practice of layering defenses to provide added protection. Defense in depth eases security by raising the cost of an attack. This system places multiple barriers between an attacker and your business-critical information resources."

It is not enough to have a good firewall. For a corporate enterprise, defense in depth at a minimum requires intrusion detection, good IT policies and security awareness training programs for employees. This report cannot help you with policies and training, but it can help you establish good firewall policies and improved perimeter defenses.

Command Line Tips

In the following sections, there will be command line instructions. All ScreenOS code will be in **bold** face type. The ***bold italic*** print specifies required information that is unique to the examples.

When entering policies from the command line, use the UP ARROW key or CTRL-B to display the previous command line input. By repeatedly tapping these keys, the command line history will be displayed. This will simplify editing policies from the command line and checking your syntax. Use the **SAVE** command to save the configuration. This will write the commands into NVRAM. It's a good practice to save the configuration regularly.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

If you need help, enter the question mark **?** at the command line. This will display all your command line options. If you make a mistake after entering in a **set** command option you can undo the setting with **unset**.

The firewall configuration can be displayed by typing:

get config

The configuration can be erased by typing:

unset all

This will erase the entire system configuration. When entering in this command, you will be prompted to confirm it. After erasing the configuration, you will need to reset.

reset

If you need to erase the configuration, do not save the configuration after issuing the unset all command. Answer "no" after issuing the reset command when prompted to save the configuration before resetting.

If you need more details concerning the command line code set, review NetScreen's Command Line Reference Guide at http://www.netscreen.com/support/downloads/NetScreen_CLI_Reference_Guide_Version_3_0.pdf.

Firewall Operation Modes

There are three modes supported by the firewall: Transparent, NAT (network address translation) and Route mode. The transparent mode operates as a layer 2 switch and uses a MAC learning table to forward packets. Transparent mode is the default operation mode. Packets that originate from the trusted network are not changed as they pass through the firewall ports. The firewall is transparent to systems communicating throught it when acting as a layer 2 switch.

In NAT mode, the firewall routes at layer 3 of the OSI model. All outgoing packets from the trusted network exiting the untrusted port are modified. The trusted host IP address is always mapped to the untrusted public IP address. The trusted IP addresses are thereby hidden by the firewall. In NAT mode, the source port is also modified using PAT or port address translation. The original source port is changed to a random source port generated by the firewall.

In route mode, the NetScreen firewall directs traffic at layer 3 and requires public IP addresses for the untrusted and trusted ports. Trusted network addresses are not changed by the firewall as the packets exit the untrusted interface.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Getting Started

Prepare a clean work area before beginning. Do not plug the firewall into the network and have a 9-pin RS-232 console cable available. If you need the pinouts for the cable, go to http://www.cablingdirectory.com/pinouts/parallelserial/RS232DB25Pinout.htm. For the purpose of this paper, we will setup the entire firewall via the command line.

Connect your workstation or laptop to the trusted firewall port using the console cable. Have all your ISP information available including your IP network, net mask and gateway information. An example of ISP supplied user information is included in Appendix B.

The firewall's trusted port arrives pre-configured with a system IP address of 192.168.1.1. Use the Hilgraeve HyperTerminal or a VT100 terminal emulator and login to the firewall. Configure your workstation network adapter to 192.168.1.2 with a 24-bit subnet mask (255.255.255.0). Open a DOS or terminal window and telnet to 192.168.1.1. The default login and password is netscreen.

Before connecting the firewall to the network, choose a new administrator login name and set it by typing:

set admin name *newadminname*

Change the default password by entering:

set admin password *GoodStr0ngPasswd!*

Password policy is a difficult topic for some organizations. If you need help choosing a strong password, review the "Setting Strong Passwords" webpage from Purdue University at http://www.adpc.purdue.edu/BSC-Pete/passwrds.htm .

Now, from your ISP-supplied network information, choose an appropriate IP address for your untrusted interface. Do not use the IP addresses provided in this example. If you have a DHCP or PPPoE connection, please consult the installation documentation.

Connect the untrusted port to your cable or DSL modem or behind your edge router if you have an E1/T1. To setup the untrusted interface and gateway, type:

set interface untrust ip *222.111.100.1 255.255.255.0*
set interface untrust gateway *222.111.100.2*

Choose an appropriate NAT network address such as 10.10.1.1 255.255.255.0. To further hide the firewall from your curious user community, set the administration management address to some other value, such as 10.10.1.111. When this is complete, set the administrator system IP address to 0.0.0.0.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

set interface trust ip *10.10.1.1 255.255.255.0*
set interface trust manage-ip *10.10.1.111*
set admin sys-ip 0.0.0.0

Save the configuration settings by typing **save**. Reset the IP address of your workstation network interface card to 10.10.1.100 255.255.255.0 with a gateway of 10.10.1.1. Ping the management port to test for good connectivity. You can now telnet into the firewall using the management IP address. If you want to access the firewall using SSH, enter this the following command which will generate the SSH-1 key for 3-DES encryption.

set scs enable

Setup on the Network

You are now ready to setup the firewall on the network. The firewall arrives pre-configured with a single inbound and outbound policy. No inbound access is permitted unless a policy is set. With the trusted and untrusted IP addresses configured, you will be able to access the public internet with the default outbound policy. Plug in the firewall to the Internet and add the following settings for basic administration.

Change the host name and SNMP name by typing:

set snmp name *newfirewall_1*

Set the domain name by typing:

set domain *yourdomain.com*

If you have an SNMP management station or are using MRTG utilization graphs, configure the following settings to enable SNMP management. Recent SNMP vulnerabilities announced by CERT such as http://www.cert.org/advisories/CA-2002-03.html have been patched. Please read the advisory and NetScreen's response http://www.netscreen.com/support/snmp.html for more information. Updated versions of ScreenOS such as release version 3.01 have been fixed.

Add the standard SNMP system contact and location information.

set admin sys-contact "*admin@yourdomain.com*"
set admin sys-location "*Your Corporate Office*"

Choose a good SNMP community string and set the device to allow traps and read-only requests. You can set these commands and your SNMP management workstation by entering:

set snmp community *GoodSNMPCOMMSTRING* Read-Only Trap-on traffic

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

set snmp host *GoodSNMPCOMMSTRING 10.10.1.101*

If the SNMP management station is at another office and connects via a VPN tunnel, the following command will need to be set.

set snmp vpn

Now, set the primary and optional secondary domain name services. Use the DNS entries provided by your ISP. The DNS host settings are used to resolve internal firewall requests such as fully qualified names used in the address book. It cannot operate as a DNS server.

set dns host dns1 *198.6.1.195*
set dns host dns2 *198.6.1.146*

The following commands will set the critical security policies to block ICMP floods, UDP floods, winnuke attack, port-scanning and IP sweeps. There are additional options available to block malicious URLs, but that is outside the scope of this report.

set firewall icmp-flood
set firewall udp-flood
set firewall winnuke
set firewall port-scan
set firewall ip-sweep

Firewall logs, event alarms and syslog messages are all important tools to administer and maintain the firewall. To successfully audit firewall events, you need this critical information available. To protect your network or home office, you need to do more than have this information available, you need to routinely monitor the logs for anomalies and security events.

Before setting up logging, configure the network time protocol so that all events are logged with accurate time stamps. This is most important when you need to correlate events in the logs from two or more devices, such as a firewall, and server log.

Set the network time updates for 60 minutes. The default setting is 5 minutes, but if you use the default and your site has low traffic, the event log will fill up with NTP messages. Adjust it as necessary for your needs. The IP address provided for NTP, in the example below, is a time server in Boulder Colorado. To find a time server in the United States, go to the NIST Internet Time Servers home page at http://www.boulder.nist.gov/timefreq/service/time-servers.html or search the Internet for one in your area. Accurate network time depends on setting your time zone offset. Adjust the timezone offset in relation to Grenwich Mean Time.

set clock ntp
set clock timezone *8*

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

set ntp server *132.163.4.102*
set ntp interval *60*

You can now setup the syslog forwarding options. You will need a syslog server to receive the messages. There are currently syslog servers available for Windows 95/98/NT/2000, Linux and Unix. Choose your flavor of OS and set one up. Substitute the IP address of your syslog server in the example below and adjust the syslog facility if necessary.

set syslog config *10.10.1.200* local0 local0 debug
set syslog enable
set syslog traffic
set syslog VPN

Enable all security alerts including IP spoofs, attack alarms, IP scans, UDP floods and login failures be sent to your email address or pager by adding the following commands.

set admin mail alert
set admin mail server-name *mailserver.yourdomain.com*
set admin mail mail-addr1 *admin1@yourdomain.com*
set admin mail mail-addr2 *adminpager@yourdomain.com*

If you want to receive the entire traffic log by email, also enter:

set admin mail traffic-log

Setup the DHCP server to provide automatic IP addresses dispensed from the firewall on the trusted network. The settings below are for forty IP addresses on the 10.10.1.0 network with DHCP lease time of 1 day. Change the settings as appropriate for your network, DNS and optional network services.

set dhcp server service
set dhcp server option lease 1440
set dhcp server option gateway *10.10.1.1*
set dhcp server option netmask *255.255.255.0*
set dhcp server option domainname *yourdomain.com*
set dhcp server option dns1 *198.6.1.146*
set dhcp server option dns2 *198.6.1.195*
set dhcp server option wins1 *10.10.1.200*
set dhcp server option wins2 *10.10.1.201*
set dhcp server ip *10.10.1.11 to 10.10.1.50*

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Good Security Practices

There are a variety of settings that will improve security. To start, disable all access to the trusted management port except secure shell and enable a single management station to access the firewall.

If you have not already enabled secure command services, type

set scs enable.

Now, remove management access to the trusted ports by entering in the unset interface commands below:

unset interface trust manage telnet
unset interface trust manage global
unset interface trust manage global-pro
unset interface trust manage web
unset interface trust manage ssl

Restricting the permitted workstations to access the firewall will improve security management. Allow access to only trusted source IP addresses and limit management requests to one or a very few devices to which physical access is restricted. For example, if your Network Operations Center is in a locked room, you should restrict management access to the NetScreen device to only those stations in the NOC. Set the management client IP address by entering:

set admin manager-ip *10.10.1.100 255.255.255.255*

Log all the packets sent directly to the firewall. This is an important setting to determine if someone is testing the firewall for vulnerabilities. By default, the firewall will discard TCP and UDP packets sent directly to the firewall if it is not listening on the destination port or service. These packets will be silently discarded. You can improve your security logging by requiring the firewall to log these discarded packets. These packets will be dropped and logged by entering:

set firewall log-self

The web management interface has a variety of features that simplify configuration. If you need to administer the firewall via the web management interface, change the firewall admin port to 8080 or another port above 1024 of your choosing. Moving the interface to a less known port will decrease inadvertent login attempts by your user community and eliminates the threat from web based denial of service attacks imposed by Trojans such as NIMDA.

set admin port *8080*

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

It is good practice to set additional filters and policies for inbound and outbound traffic. Simple egress filters can be made to limit the allowed outbound traffic and monitor traffic typically reserved for administrative duties such as Telnet, SSH and Ping. The following filters have been setup into two groups. The first group is permitted client protocols and the second is permitted admin protocols that are logged and monitored.

Before creating the policy, the trusted network address must be established. Create the address book entry for the local network by typing:

set address trust "*Local LAN*" *10.10.1.0 255.255.255.0*

The permitted client protocols can now be established. Choose protocols that are in accordance with your organizations needs or based on your security policy. For this example, HTTP, DNS, secure HTTP, FTP, NTP, NNTP and SMTP mail have been chosen.

set group service "*ClientProtocols*" comment "*Permitted Protocols*"
set group service "*ClientProtocols*" add HTTP
set group service "*ClientProtocols*" add DNS
set group service "*ClientProtocols*" add HTTPS
set group service "*ClientProtocols*" add FTP
set group service "*ClientProtocols*" add NTP
set group service "*ClientProtocols*" add NNTP
set group service "*ClientProtocols*" add MAIL

For the allowed administrative protocols, Ping, SSH, Telnet and IRC have been chosen. These examples are not applicable to all organizations. Some organizations may prefer to deny outgoing access to IRC chat groups.

The POP3 protocol has been added to the administrative group in order to monitor unencrypted mail. This is a helpful setting if you have a security policy that does not allow unencrypted mail.

set group service "*AdminProtocols*" comment "*Permitted Protocols - logged* "
set group service "*AdminProtocols*" add PING
set group service "*AdminProtocols*" add SSH
set group service "*AdminProtocols*" add TELNET
set group service "*AdminProtocols*" add IRC
set group service "*AdminProtocols*" add POP3

The custom service groups have now been created. Now, you can create the actual incoming and outgoing policy for client protocols by typing:

set policy outgoing "*Local LAN*" "Outside Any" "*ClientProtocols*" Permit

You can now create the permitted administrative protocol group that is logged.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

set policy outgoing "*Local LAN*" "Outside Any" "*AdminProtocols*" Permit log

You have now successfully created two outgoing policies. As with any policy-based firewall, you will have to put the policies in the proper order to ensure that the firewall performs as directed. The default outgoing deny policy uses policy ID 0. You will need to display the policies and then re-order them.

get policy

The get policy command will display the policies in the order they are executed. To move the default policy after the recently created policies, type:

set policy move 0 after *2*

If you have created additional policies besides those in the example above, you will need to move the policy after the last numbered policy ID.

Now, for better security, change the default outgoing permit policy to deny all outgoing traffic except the traffic that has been previously allowed. Logging the output to an event file and syslog server will improve your forensic capability and help you understand what protocols and services are being used on the network. To set this, type:

set policy outgoing "Inside Any" "Outside Any" "ANY" Deny log

By default, the firewall is also set with an implicit deny policy on all inbound traffic. This can be improved by setting an explicit incoming deny policy that logs all event traffic. This will allow you to log all traffic that is sent directly to the firewalls untrusted port. To do this type:

set policy incoming "Outside Any" "All Virtual IPs" "ANY" Deny log

Creating a VPN Tunnel

A virtual private network tunnel is not an actual tunnel. It is encrypted traffic that is authorized to pass through the firewall. According to IETF RFC's 2402 and 2406, IPSEC uses two protocols. These are encapsulation security payload (ESP) using protocol 50 and authentication header (AH) using protocol 51. IPSEC encryption can be performed using algorithms such as DES, DES and AES while the data is authenticated using algorithms like HMAC-MD5 and HMAC_SHA.

The NetScreen 5XP firewall can support multiple types of VPN, such as LAN-to-LAN with static IP addresses, LAN-to-LAN with dynamic and static IP addresses, and Dialup-to-LAN. The following section will show how to setup a VPN connection using static IP addresses with 3DES encryption and SHA-1 authentication.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

For the purpose of this example, the second NetScreen firewall will be setup identical to the first with the exception of the untrusted and trusted firewall ports, DHCP server and the hostname. The second firewall will use:

set interface untrust ip *222.111.100.2 255.255.255.0*
set interface untrust gateway *222.111.100.1*
set snmp name *newfirewall_2*
set interface trust ip *10.10.2.1 255.255.255.0*
set interface trust manage-ip *10.10.2.111*
set admin sys-ip 0.0.0.0
set address trust "*Local LAN" 10.10.2.0 255.255.255.0*

Before beginning, decide on your VPN settings. This example will use aggressive mode settings for the Phase I proposal set for 3DES and SHA-1. The preshared key will be set to *ourkey123*. The Phase II proposal will also use 3DES and SHA-1. In Phase I and II, the firewalls setup a secure encrypted communication channel by creating a shared symmetric key using the Diffie-Hellman key exchange algorithm.

On newfirewall_1, create an address book entry for the newfirewall_2 network.

set address untrust "Local LAN FW2" 10.10.2.0 255.255.255.0

Now, enter the tunnel gateway for the Phase I proposal. The Phase I proposal will require a preshared key. This alpha-numeric key is required on each firewall to create the SHA-1 hash used to authenticate the tunnel. The minimum recommended key length is eight characters with a maximum of thirty-two.

set ike gateway "*p1-FW2*" ip *222.111.100.2* Aggr preshare "*ourkey123*" proposal "pre-g2-3des-sha"

On newfirewall_1 the Phase II proposal will need to be set, type:

set vpn "*p2-FW2*" id 1 gateway "*p1-FW2*" no-replay tunnel idletime 0 proposal "g2-esp-3des-sha"

If we take a closer look at the policies set above, there are two settings that need some explanations. The first is the g2-esp-3des-sha setting. The g2 component signifies that the tunnel is using perfect forward secrecy using Diffie-Hellman key exchange group 2 with the later part specifying 3DES encryption and SHA authenticaton. For more information concerning Diffie-Hellman key exchange, read RFC 2786 at http://www.ietf.org/rfc/rfc2786.txt or "Diffie-Hellman Key Exchange – A Non-Mathematician's Explanation" by Keith Palmgren at http://www.netip.com/articles/keith/diffie-helman.htm . The second setting we'll look at is no-replay, this enables replay protection so that a session cannot resend traffic already authenticated through the firewall tunnel.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

After the Phase I & II proposals are set, the inbound and outbound policies will need to be established.

set policy incoming "*Local LAN FW2*" "*Local LAN*" "ANY" Tunnel vpn "*p2-FW2*" log
set policy outgoing "*Local LAN*" "*Local LAN FW2*" "ANY" Tunnel vpn "*p2-FW2*" log

The same steps will need to be taken on newfirewall_2. Create the untrusted address book entry for the newfirewall_1 network, make the Phase 1 & II proposals and corresponding incoming and outgoing policies.

set ike gateway "*p1-FW1*" ip 222.111.100.1 Aggr preshare "*ourkey123*" proposal "pre-g2-3des-sha"

set vpn "*p2-FW1*" id 1 gateway "*p1-FW1*" no-replay tunnel idletime 0 proposal "g2-esp-3des-sha"

set policy incoming "*Local LAN FW1*" "*Local LAN*" "ANY" Tunnel vpn "*p2-FW1*" log

set policy outgoing "*Local LAN*" "*Local LAN FW1"* "ANY" Tunnel vpn "*p2-FW1*" log

There is one step left before the tunnel can be established. The outgoing policies will need to be re-ordered. Display all the policies using the **get policy** command, then move policy ID 0 after the last policy. Use the following on each firewall, if you have added additional policies, choose the last policy ID and type:

set policy move 0 after *6*

You can now test the tunnel by pinging from one trusted network to the other. Ping the remote NetScreen trusted IP address on newfirewall_2 from the trusted port by typing:

ping *10.10.1.111* from trust

The complete firewall configurations are included in Appendix A. If there are problems with your firewall tunnel connectivity, check the configuration against the appendix.

Summary

The NetScreen firewall is an excellent network appliance that can easily adapt and scale to fit any architecture. The ScreenOS software is simple to configure if you use the web GUI. Many engineers prefer to use the command line - this report is written for those engineers and other interested technologists.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Appendix A

Below is the complete configuration for the two firewalls (newfirewall_1 & newfirewall_2). The configuration can be displayed by typing **get config**.

newfirewall_1-> get config

```
Total Config size 4803:
set auth type 0
set auth timeout 10
set clock ntp
set clock "timezone" 8
set admin format dos
set admin name "newadminname"
set admin password nMw5AcrFF7uHcSqD+sYBu4Jt3xKUwn
set admin manager-ip 10.10.1.100 255.255.255.0
set admin sys-ip 0.0.0.0
set admin port 8080
set admin sys-contact "admin@yourdomain.com"
set admin sys-location "Your Corporate Office"
set admin mail alert
set admin mail server-name mailserver.yourdomain.com
set admin mail mail-addr1 admin1@yourdomain.com
set admin mail mail-addr2 adminpager@yourdomain.com
set admin mail traffic-log
set admin auth timeout 10
set admin auth type Local
set ip tftp retry 10
set ip tftp timeout 2
set interface trust ip 10.10.1.1 255.255.255.0
set interface untrust ip 222.111.100.1 255.255.255.0
set interface untrust gateway 222.111.100.2
set interface trust manage-ip 10.10.1.111
set interface trust manage ping
set interface trust manage scs
unset interface trust manage telnet
set interface trust manage snmp
unset interface trust manage global
unset interface trust manage global-pro
unset interface trust manage ssl
unset interface trust manage web
unset interface trust ident-reset
unset interface untrust manage ping
unset interface untrust manage scs
unset interface untrust manage telnet
unset interface untrust manage snmp
unset interface untrust manage global
```

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

```
unset interface untrust manage global-pro
unset interface untrust manage ssl
unset interface untrust manage web
unset interface untrust ident-reset
set flow mac-flooding
set flow check-session
set domain yourdomain.com
set hostname newfirewall_1
set ntp server 132.163.4.102
set ntp interval 60
set address untrust "Local LAN FW2" 10.10.2.0 255.255.255.0
set address trust "Local LAN" 10.10.1.0 255.255.255.0
set syn-threshold 200
set firewall tear-drop
set firewall syn-flood
set firewall ip-spoofing
set firewall ping-of-death
set firewall src-route
set firewall land
set firewall icmp-flood
set firewall udp-flood
set firewall winnuke
set firewall port-scan
set firewall ip-sweep
unset firewall applet
unset firewall bypass-others-ipsec
unset firewall bypass-non-ip
set firewall log-self
unset firewall session-threshold source-ip-based
set snmp community GoodSNMPCOMMSTRING Read-Only Trap-on traffic
set snmp host GoodSNMPCOMMSTRING 10.10.1.101
set snmp location "Your Corporate Office"
set snmp contact "admin@yourdomain.com"
set snmp name "newfirewall_1"
set snmp vpn
set group service "ClientProtocols" comment "Permitted Protocols"
set group service "ClientProtocols" add "HTTP"
set group service "ClientProtocols" add "DNS"
set group service "ClientProtocols" add "HTTPS"
set group service "ClientProtocols" add "FTP"
set group service "ClientProtocols" add "NTP"
set group service "ClientProtocols" add "NNTP"
set group service "ClientProtocols" add "MAIL"
set group service "AdminProtocols" comment "Permitted Protocols-logged"
set group service "AdminProtocols" add "PING"
set group service "AdminProtocols" add "SSH"
```

© SANS Institute 2002, Author retains full rights.

```
set group service "AdminProtocols" add "TELNET"
set group service "AdminProtocols" add "IRC"
set group service "AdminProtocols" add "POP3"
set ike gateway "p1-FW2" ip 222.111.100.2 Aggr preshare "ourkey123" proposal "pre-
g2-3des-sha"
set ike policy-checking
set ike respond-bad-spi 1
set vpn "p2-FW2" id 1 gateway "p1-FW2" no-replay tunnel idletime 0 proposal "g2-
esp-3des-sha"
set l2tp default auth local
set l2tp default ppp-auth any
set l2tp default radius-port 1645
set ike id-mode subnet
set traffic-shaping ip_precedence 7 6 5 4 3 2 1 0
set policy id 1 outgoing "Local LAN" "Outside Any" "ClientProtocols" Permit
set policy id 2 outgoing "Local LAN" "Outside Any" "AdminProtocols" Permit log
set policy id 5 incoming "Outside Any" "All Virtual IPs" "ANY" Deny log
set policy id 4 incoming "Local LAN FW2" "Local LAN" "ANY" Tunnel vpn "p2-FW2"
id 2 log
set policy id 6 outgoing "Local LAN" "Local LAN FW2" "ANY" Tunnel vpn "p2-FW2" i
d 2 log
set policy id 0 outgoing "Inside Any" "Outside Any" "ANY" Deny log
set dhcp server service
set dhcp server option lease 1440
set dhcp server option gateway 10.10.1.1
set dhcp server option netmask 255.255.255.0
set dhcp server option domainname yourdomain.com
set dhcp server option dns1 198.6.1.146
set dhcp server option dns2 198.6.1.195
set dhcp server option wins1 10.10.1.200
set dhcp server option wins2 10.10.1.201
set dhcp server ip 10.10.1.11 to 10.10.1.50
set syslog config 10.10.1.200 local0 local0 debug
set syslog enable
set syslog traffic
set syslog VPN
set firewall ip-sweep threshold 30000
set scs enable
set pki authority default scep mode "auto"
set pki x509 default cert-path partial
set dns host dns1 198.6.1.195
set dns host dns2 198.6.1.146
```

newfirewall_2-> get config

```
Total Config size 4803:
set auth type 0
```

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

```
set auth timeout 10
set clock ntp
set clock "timezone" 8
set admin format dos
set admin name "newadminname"
set admin password nMw5AcrFF7uHcSqD+sYBu4Jt3xKUwn
set admin manager-ip 10.10.1.100 255.255.255.0
set admin sys-ip 0.0.0.0
set admin port 8080
set admin sys-contact "admin@yourdomain.com"
set admin sys-location "Your Corporate Office"
set admin mail alert
set admin mail server-name mailserver.yourdomain.com
set admin mail mail-addr1 admin1@yourdomain.com
set admin mail mail-addr2 adminpager@yourdomain.com
set admin mail traffic-log
set admin auth timeout 10
set admin auth type Local
set ip tftp retry 10
set ip tftp timeout 2
set interface trust ip 10.10.2.1 255.255.255.0
set interface untrust ip 222.111.100.2 255.255.255.0
set interface untrust gateway 222.111.100.1
set interface trust manage-ip 10.10.2.111
set interface trust manage ping
set interface trust manage scs
unset interface trust manage telnet
set interface trust manage snmp
unset interface trust manage global
unset interface trust manage global-pro
unset interface trust manage ssl
unset interface trust manage web
unset interface trust ident-reset
unset interface untrust manage ping
unset interface untrust manage scs
unset interface untrust manage telnet
unset interface untrust manage snmp
unset interface untrust manage global
unset interface untrust manage global-pro
unset interface untrust manage ssl
unset interface untrust manage web
unset interface untrust ident-reset
set flow mac-flooding
set flow check-session
set domain yourdomain.com
set hostname newfirewall_2
```

© SANS Institute 2002, Author retains full rights.

```
set ntp server 132.146.4.102
set ntp interval 60
set address untrust "Local LAN FW1" 10.10.1.0 255.255.255.0
set address trust "Local LAN" 10.10.2.0 255.255.255.0
set syn-threshold 200
set firewall tear-drop
set firewall syn-flood
set firewall ip-spoofing
set firewall ping-of-death
set firewall src-route
set firewall land
set firewall icmp-flood
set firewall udp-flood
set firewall winnuke
set firewall port-scan
set firewall ip-sweep
unset firewall applet
unset firewall bypass-others-ipsec
unset firewall bypass-non-ip
set firewall log-self
unset firewall session-threshold source-ip-based
set snmp community GoodSNMPCOMMSTRING Read-Only Trap-on traffic
set snmp host GoodSNMPCOMMSTRING 10.10.1.101
set snmp location "Your Corporate Office"
set snmp contact "admin@yourdomain.com"
set snmp name "newfirewall_2"
set snmp vpn
set group service "ClientProtocols" comment "Permitted Protocols"
set group service "ClientProtocols" add "HTTP"
set group service "ClientProtocols" add "DNS"
set group service "ClientProtocols" add "HTTPS"
set group service "ClientProtocols" add "FTP"
set group service "ClientProtocols" add "NTP"
set group service "ClientProtocols" add "NNTP"
set group service "ClientProtocols" add "MAIL"
set group service "AdminProtocols" comment "Permitted Protocols -logged"
set group service "AdminProtocols" add "PING"
set group service "AdminProtocols" add "SSH"
set group service "AdminProtocols" add "TELNET"
set group service "AdminProtocols" add "IRC"
set group service "AdminProtocols" add "POP3"
set ike gateway "p1-FW1" ip 222.111.100.1 Aggr preshare "ourkey123" proposal "pre-
g2-3des-sha"
set ike policy-checking
set ike respond-bad-spi 1
set vpn "p2-FW1" id 1 gateway "p1-FW1" no-replay tunnel idletime 0 proposal "g2-
```

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

```
esp-3des-sha"
set l2tp default auth local
set l2tp default ppp-auth any
set l2tp default radius-port 1645
set ike id-mode subnet
set traffic-shaping ip_precedence 7 6 5 4 3 2 1 0
set policy id 1 outgoing "Local LAN" "Outside Any" "ClientProtocols" Permit
set policy id 2 outgoing "Local LAN" "Outside Any" "AdminProtocols" Permit log
set policy id 5 incoming "Outside Any" "All Virtual IPs" "ANY" Deny log
set policy id 4 incoming "Local LAN FW1" "Local LAN" "ANY" Tunnel vpn "p2-FW1"
id 2 log
set policy id 6 outgoing "Local LAN" "Local LAN FW1" "ANY" Tunnel vpn "p2-FW1" i
d 2 log
set policy id 0 outgoing "Inside Any" "Outside Any" "ANY" Permit log
set dhcp server service
set dhcp server option lease 1440
set dhcp server option gateway 10.10.2.1
set dhcp server option netmask 255.255.255.0
set dhcp server option domainname yourdomain.com
set dhcp server option dns1 198.6.1.146
set dhcp server option dns2 198.6.1.195
set dhcp server option wins1 10.10.2.200
set dhcp server option wins2 10.10.2.201
set dhcp server ip 10.10.2.11 to 10.10.2.50
set syslog config 10.10.1.200 local0 local0 debug
set syslog enable
set syslog traffic
set syslog VPN
set firewall ip-sweep threshold 30000
set scs enable
set pki authority default scep mode "auto"
set pki x509 default cert-path partial
set dns host dns1 198.6.1.195
set dns host dns2 198.6.1.146
```

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Appendix B
The following form is only an example.

Dear XXX ISP customer 5551212:

We are happy to announce that your Internet connection is now working and has been fully tested. This letter contains important information about your on-going relationship with XXX ISP. The Customer Installations department operates between 8 AM and 7 PM ET (13h00GMT-5 and 24h00GMT-5), Monday through Friday (excluding holidays). If you are working with an installation engineer based in Europe, their hours are between 8 AM and 6 PM GMT. If you require assistance outside of these hours, you will need to schedule this with your engineer.

Customer IP Address : 65.142.226.2
Customer internet gateway : 65.142.226.1

Subnet Mask: 255.255.255.248

DNS1: 198.6.1.3
DNS2: 198.6.1.4

SMTP gateway: smtp.ispdomain.com
POP3 gateway: pop3.ispdomain.com

News server: nntp.ispdomain.com

To add your host to the DNS server, call xxx-555-1212 during normal business hours or send an email to help@ispdoman.com.

© SANS Institute 2002, Author retains full rights.

Sources

Avolio, Frederick M. "Best Practices in Network Security." URL: http://www.networkcomputing.com/1105/1105f2.html. 20 March 2000. (March 2002)

"CERT Advisory CA-2002-03 Multiple Vulnerabilities in Many Implementations of the Simple Network Management Protocol (SNMP)." URL: http://www.cert.org/advisories/CA-2002-03.html. 12 February 2002. (March 2002)

Denning, Dorothy E. Information Warfare and Security. Addison Welsey, 1999. Part 1

"Diffie-Helman USM Key Management Information Base and Textual Convention." URL: http://www.ietf.org/rfc/rfc2786.txt. March 2000. (April 2002)

Implementing NetScreen Security Solutions. Student Guide Version 2.6b, NetScreen Technologies, 2001 Chapters 11-13

"IP Authentication Header." URL: http://www.ietf.org/rfc/rfc2402.txt. November 1998. (April 2002)

"IP Encapsulation Security Payload." URL: http://www.ietf.org/rfc/rfc2406.txt. November 1998. (April 2002)

"IP Security Protocol (ipsec)." URL: http://www.ietf.org/html.charters/ipsec-charter.html. 5 Feb 2002. (April 2002)

"NetScreen-5XP Installers Guide." URL: http://www.netscreen.com/support/downloads/NS-5XP_Install.pdf. ScreenOS 3.0.0 Rev. A. (March 2002)

"NetScreen CLI Reference Guide version 3.0." URL: http://www.netscreen.com/support/downloads/NetScreen_CLI_Reference_Guide_Version_3_0.pdf. ScreenOS3.0.0 Rev. B. (April 2002)

"NetScreen Response to: CERT Advisory CA-2002-03 "Multiple Vulnerabilities in Many Implementations of the Simple Network Management Protocol (SNMP)"." URL: http://www.netscreen.com/support/snmp.html. 13 February 2002. (March 2002)

"Network Security Policy: Best Practices White Paper." URL: http://www.cisco.com/warp/public/126/secpol.html. Document ID 13601, 9 April 2002. (April 2002)

"NIST Internet Time Servers." URL: http://www.boulder.nist.gov/timefreq/service/time-servers.html. (March 2002)

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Palmgren, Keith. "Diffie-Hellman Key Exchange – A Non-Mathematician's Explanation" URL: http://www.netip.com/articles/keith/diffie-helman.htm. 21 February 2002. (April 2002)

Parker, Eric. "NetScreen 5." 24 July 2001. URL: http://www.mindsec.com/reviews/ns5.html. (March 2002)

Paul, Brooke. "Building an In-Depth Defense." Network Computing. 9 July 2001. URL: http://www.networkcomputing.com/1214/1214ws1.html. (March 2002)

"RS232 Cable Pinout." Cabling Directory.com. URL: http://www.cablingdirectory.com/pinouts/parallelserial/RS232DB9Pinout.htm. (April 2002)

SANS Security Essentials I: Information Security, The Big Picture. SANS Institute, 2001

SANS Incident Handling Step By Step. SANS Institute, 2000

"Secure Hash Standard." URL: http://www.itl.nist.gov/fipspubs/fip180-1.htm. FIPS PUB 180-1. 11 May 1993. (March 2002)

"Setting Strong Passwords." URL: http://www.adpc.purdue.edu/BSC-Pete/passwrds.htm. (March 2002)

Stanger, James and Lane, Patrick T. Hack Proofing Linux. Syngress Media, 2001

Technical Publications Dept. "NetScreen Getting Started with NetScreen-5XP Quick Start." NetScreen Technologies. August 2001

Warren, Steven. "Design the best security topology for your firewall." URL: http://www.zdnet.co.uk/news/specials/2000/10/enterprise/techrepublic/2002/10/article002.html. 11 March 2002 (March 2002)

© SANS Institute 2002, Author retains full rights.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: August 31st, 2015

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Crystal City 2015	Crystal City, VAUS	Sep 08, 2015 - Sep 13, 2015	Live Event
SANS Network Security 2015	Las Vegas, NVUS	Sep 12, 2015 - Sep 21, 2015	Live Event
SANS Seoul 2015	Seoul, KR	Sep 14, 2015 - Sep 19, 2015	Live Event
Data Breach Investigation Summit & Training	Dallas, TXUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Baltimore 2015	Baltimore, MDUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Perth 2015	Perth, AU	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Tallinn 2015	Tallinn, EE	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS ICS Amsterdam 2015	Amsterdam, NL	Sep 22, 2015 - Sep 28, 2015	Live Event
SANS Bangalore 2015	Bangalore, IN	Sep 28, 2015 - Oct 17, 2015	Live Event
SANS DFIR Prague 2015	Prague, CZ	Oct 05, 2015 - Oct 17, 2015	Live Event
SANS Seattle 2015	Seattle, WAUS	Oct 05, 2015 - Oct 10, 2015	Live Event
SANS Tysons Corner 2015	Tysons Corner, VAUS	Oct 12, 2015 - Oct 17, 2015	Live Event
SOS: SANS October Singapore 2015	Singapore, SG	Oct 12, 2015 - Oct 24, 2015	Live Event
SANS Gulf Region 2015	Dubai, AE	Oct 17, 2015 - Oct 29, 2015	Live Event
SANS Cyber Defense San Diego 2015	San Diego, CAUS	Oct 19, 2015 - Oct 24, 2015	Live Event
SANS Tokyo Autumn 2015	Tokyo, JP	Oct 19, 2015 - Oct 31, 2015	Live Event
SANS South Florida 2015	Fort Lauderdale, FLUS	Nov 09, 2015 - Nov 14, 2015	Live Event
SANS Sydney 2015	Sydney, AU	Nov 09, 2015 - Nov 21, 2015	Live Event
SANS London 2015	London, GB	Nov 14, 2015 - Nov 23, 2015	Live Event
Pen Test Hackfest Summit & Training	Alexandria, VAUS	Nov 16, 2015 - Nov 23, 2015	Live Event
SANS Hyderabad 2015	Hyderabad, IN	Nov 24, 2015 - Dec 04, 2015	Live Event
SANS Cape Town 2015	Cape Town, ZA	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS San Francisco 2015	San Francisco, CAUS	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS Milan 2015	OnlineIT	Sep 07, 2015 - Sep 12, 2015	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced