

Application Note: Hardening Netscreen Firewalls

Version 1.2, 07/18/2002

Stephen Gill
E-mail: gillsr@cymru.com
Published: 07/10/2002

Contents

Introduction	2
Assumptions	3
Topology	3
Configuration	5
Logging.....	5
Management.....	6
Time Synchronization	9
High Availability	9
VPN	11
Policies	14
Traffic Screening	16
Miscellaneous.....	18
Conclusion	18
References	18
Appendix A	19

Introduction

Given the increased visibility and importance of security aimed at the protection of intellectual property and business continuity, modern networks must be well guarded against the widespread threats typically encountered on the Internet. These threats range from the most simple to the most Distributed Denial of Service (DDoS) attacks. The security challenge presented is to block unwanted traffic while allowing normal business to operate seamlessly.

In many of today's enterprise architectures, firewalls reside at the network edge policing access to and from network internals. Unfortunately, firewalls are typically the sole guardians of the castle. Rather than employing additional methods of security at the server and network level, firewalls are expected to do it all. This is clearly not the best approach.

One of the most effective ways to keep out unwanted traffic is to incorporate a layered approach to security. This strategy encompasses several fronts, or major lines of defense within the network. Larger generic attacks can be mitigated at the border routers, medium to large attacks on the firewalls and load balancers and small to medium attacks at the host or server level.

In order to attain the funneled granular filtering approach to network security, unwanted traffic must be blocked as far as possible upstream while maintaining reliability and performance. In practice, routers are not built for security, firewalls are not designed for routing throughput and servers are not deployed as distribution points. In many ways, the uses of

routers and firewalls coincide, but by drawing from the most effective functions of these devices and bringing them together, a more reliable, secure and robust network can be fashioned.

Since Netscreen firewalls are dedicated hardware appliances with a proprietary operating system, one might question what really can be done to harden them. Often firewalls are deployed with the mistaken assumption that they will fully protect users from most security threats. The truth is that much care must be taken when crafting a firewall security policy, and merely deploying a firewall does not preclude a network from certain security exposures.

Firewalls should not be used as the first and only line of network defense. That said, the focus of this paper is to guide the Netscreen administrator through the process of hardening and standardizing his or her firewall configuration by employing current industry security best practices. Auditing firewall configurations is a key step in the funneled enclave approach to network security.

Assumptions

A few assumptions worth noting are made by this document. Firstly, we assume that the reader is familiar with general security and Netscreen specific concepts. More specific information and documentation on configuring Netscreen firewalls can be obtained from www.netscreen.com.

Secondly, we assume that the configuration described herein is specific to our test network topology and should be adapted to individual network requirements. Certain configuration parameters can be easily transferred to other networks, while others may require additional customization and fine tuning.

Finally, we note that the configurations are written from the perspective of the Netscreen 500s in the hub site running ScreenOS version 3.1. At the time of this writing, version 3.1 is the most recent level of code aside from the soon to be released, ScreenOS 4.0.

Topology

Before delving into the details of our recommended hardening measures, we present a topology diagram on which the configuration details are based.

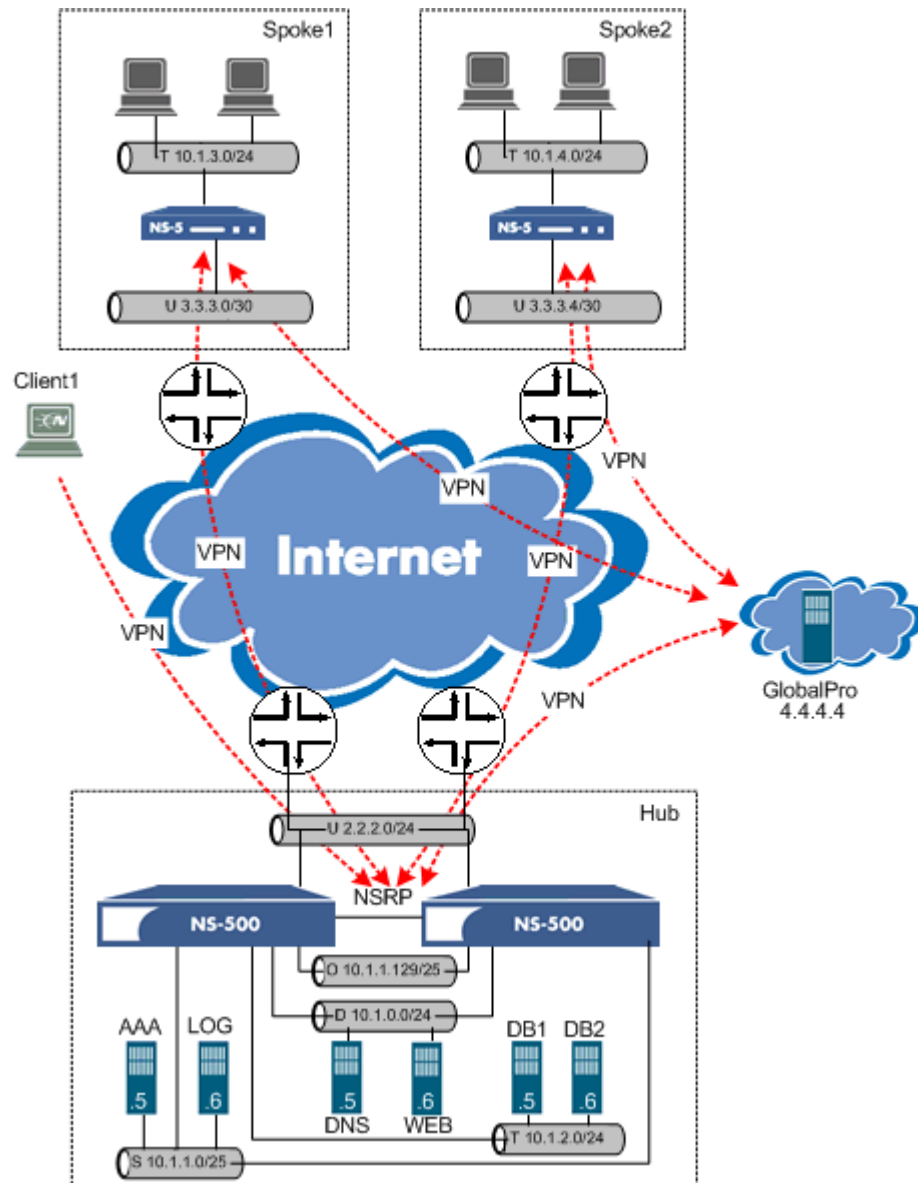


Figure 1 - Netscreen Topology

The topology in Figure 1 includes one hub site and two spoke sites. The hub site contains web servers, management servers, and acts as the VPN termination point at the Netscreen 500s for Netscreen VPN Clients and all the spoke sites. Each spoke site consists of internal servers and a Netscreen 5XP firewall. Global Pro, a remote tool for centralized reporting and policy management, resides in a separate cloud. All relevant IP networks have been included in the diagram and are summarized below:

Network	Description
2.2.2.0/24	hub-untrust
3.3.3.0/30	spoke1-untrust
3.3.3.4/30	spoke2-untrust
10.1.0.0/24	hub-dmz

10.1.1.0/25	hub-sec
10.1.1.128/25	hub-oob
10.1.2.0/24	hub-trust
10.1.3.0/24	spoke1-trust
10.1.4.0/24	spoke2-trust

Table 1 - Network Descriptions

Configuration

The configurations below have been subdivided into several sections for ease of readability. Each sub-section contains helpful descriptive information about the commands along with occasional troubleshooting hints.

ScreenOS allows for both WEB and CLI forms of configuration entry. However, the configurations presented in this paper are all text-based for the following reasons:

- configuration statements are easier to read and understand
- some commands are only available on the CLI interface
- configurations are easy to modify, replicate, and automate
- more extensive troubleshooting can be performed via the CLI
- text configurations are easier to document than screen captures

Logging

Firewall logging enables the security administrator to perform several important functions including, historical flow tracking, event correlation, and network troubleshooting. A Netscreen firewall can be configured to forward its traffic logs to a remote syslog server of choice. Syslog uses UDP port 512 and comes with most, if not all UNIX distributions.

Below we, specify the syslog server IP address, and local0 as the facility, and severity levels. Only messages with notice priority and higher will be sent.

```
set syslog config 10.1.1.6 local0 local0 notice
```

The next two commands will enable syslog and configure the firewall to forward traffic logs to the syslog server:

```
set syslog enable  
set syslog traffic
```

Traffic that terminates at the firewall is not logged by default. To turn this feature on including IKE and SNMP traffic, use the following commands:

```
set firewall log-self  
set firewall log-self ike  
set firewall log-self snmp
```

The active syslog settings can be verified with the '*get syslog config*' command. Different log levels can be set on a per device basis such as

the console, email, etc... However, the default system parameters are acceptable in this case. These settings are viewed with the `'get log setting'` command. The firewall log settings will show up in the output of the `'get firewall'` command.

Specific log entries can either be viewed on the syslog server, or at the firewall. Firewall traffic entries are viewed through the `'get log self'` command which can be further restricted by IP address, flow duration, service, and more. Finally, policy traffic logs are viewed with the `'get log traffic'` command, which also can be further restricted by IP address, flow duration, service, policy number, and more. A policy must be configured to log on a match for an entry to show up in the traffic logs. The syntax for configuring policy logging is presented in the policy section later in this document.

To receive a summary of all traffic logs via SMTP, an administrative e-mail address and mail server are specified below. The administrator may chose to bypass this step if traffic logs are excessive. Instead, a better option may be to parse the logs received on the syslog server with network specific scripts.

```
set admin mail server-name 10.1.1.6
set admin mail mail-addr1 gillsr@yahoo.com
set admin mail traffic-log
```

Management

System services are enabled on a per interface basis. For each management service that is enabled, an implicit policy is created on the firewall that allows the configured management servers to connect. Ping is the only exception to this rule as anyone on that side of the firewall will be able to ping the firewall interface if it is enabled. If no management servers are listed, then access to these services will not be restricted.

The following configuration statements assign the management interface an IP address, enable ping, ssh, snmp, web, and ssl. All unnecessary management services are disabled on this interface. By design, no traffic can be routed through this special out of band management interface.

```
set interface mgt ip 10.1.1.129/25
set interface mgt manage ping
set interface mgt manage scs
unset interface mgt manage telnet
set interface mgt manage snmp
unset interface mgt manage global
set interface mgt manage global-pro
set interface mgt manage ssl
set interface mgt manage web
```

Next we place the first Ethernet interface in the trust zone, assign it an IP address, set it to route mode and enable ping. All unnecessary management services are disabled on this interface.

```
set interface ethernet1/1 zone trust
```

```
set interface ethernet1/1 ip 10.1.2.1/24
set interface ethernet1/1 route
set interface ethernet1/1 manage ping
unset interface ethernet1/1 manage scs
unset interface ethernet1/1 manage telnet
unset interface ethernet1/1 manage snmp
unset interface ethernet1/1 manage global
unset interface ethernet1/1 manage global-pro
unset interface ethernet1/1 manage ssl
unset interface ethernet1/1 manage web
unset interface ethernet1/1 ident-reset
```

The second Ethernet interface will be used for the security servers. We must define our zone name (security) since this is not one of the predefined zones. We assign the interface to the security zone, give it an IP address, and enable ping, ssh, and global-pro. All unnecessary management services are disabled on this interface.

```
set zone name sec
set zone sec vrouter trust-vr
set interface ethernet1/2 zone sec
set interface ethernet1/2 ip 10.1.1.1/25
set interface ethernet1/2 route
set interface ethernet1/2 manage ping
set interface ethernet1/2 manage scs
unset interface ethernet1/2 manage telnet
unset interface ethernet1/2 manage snmp
unset interface ethernet1/2 manage global
set interface ethernet1/2 manage global-pro
unset interface ethernet1/2 manage ssl
unset interface ethernet1/2 manage web
unset interface ethernet1/2 ident-reset
```

Enabling the scs service on an interface will allow access via TCP port 22 to that interface, but the service must also be enabled globally like so:

```
set scs enable
```

It is very important not to rely on default settings when enabling SNMP. Here we allow read-only access from our utility server using a predefined community string. SNMP traps will also be forwarded to the same server.

```
set snmp community sh0wm3th3$ Read-Only Trap-on
set snmp host sh0wm3th3$ 10.1.1.6
```

Below we also configure the system name, contact, and location information to set the corresponding SNMP variables. The system hostname and domain are also configured.

```
set snmp contact "Stephen Gill"
set snmp location "Test Lab"
set snmp name "NS500"
set hostname ns500
set domain site.com
```

Netscreen Global-Pro is also used to manage the firewalls in our topology. Therefore we enable this feature along with all the reporting features it provides. Since Global-Pro traffic is not encrypted by default through the NSP protocol, we enable the VPN setting to source traffic from a secured interface.

```
set global-pro enable
set global-pro vpn
set global-pro config primary 4.4.4.4
```

```

set global-pro policy-manager primary host 4.4.4.4
set global-pro report proto-dist enable
set global-pro report ethernet-stat enable
set global-pro report attack-stat enable
set global-pro report flow-stat enable
set global-pro report policy-stat enable
set global-pro report alarm-traffic enable
set global-pro report alarm-attack enable
set global-pro report alarm-other enable
set global-pro report log-config enable
set global-pro report log-info enable
set global-pro report log-self enable
set global-pro report log-traffic enable

```

Next, we place the third and fourth Ethernet interfaces in their respective zones, configure their IP addresses and enable ping only.

```

set interface ethernet2/1 zone untrust
set interface ethernet2/1 ip 2.2.2.1/24
set interface ethernet2/1 manage ping
unset interface ethernet2/1 manage scs
unset interface ethernet2/1 manage telnet
unset interface ethernet2/1 manage snmp
unset interface ethernet2/1 manage global
unset interface ethernet2/1 manage global-pro
unset interface ethernet2/1 manage ssl
unset interface ethernet2/1 manage web
unset interface ethernet2/1 ident-reset
set interface ethernet2/2 zone dmz
set zone dmz vrouter untrust-vr
set interface ethernet2/2 ip 10.1.0.1/24
set interface ethernet2/2 manage ping
unset interface ethernet2/2 manage scs
unset interface ethernet2/2 manage telnet
unset interface ethernet2/2 manage snmp
unset interface ethernet2/2 manage global
unset interface ethernet2/2 manage global-pro
unset interface ethernet2/2 manage ssl
unset interface ethernet2/2 manage web
unset interface ethernet2/2 ident-reset

```

The default username and password should not be left unchanged. Here we changed from the standard username and password of Netscreen to something a bit more secure.

```

set admin name "admin"
set admin password nEbYCyrbAZGKcQHHDsEAioItl1DIIn

```

Aside the local username database, RADIUS can also be enabled to perform device authentication. Following are the settings for enabling RADIUS and configuring the host, port, shared secret, and timeout settings. Keep in mind that the local username database will be consulted despite a negative response from the RADIUS server.

```

set admin auth type radius
set admin auth server-name 10.1.1.5
set admin auth secret <secret>
set admin auth radius-port 1812
set admin auth timeout 10

```

User authentication settings are stored apart from system authentication. Policies may restrict or allow access to particular network devices based on users. Here we also use RADIUS (type 1) for user authentication.

```

set auth type 1
set auth server-name 10.1.1.5
set auth secret <secret>
set auth radius-port 1812
set auth timeout 10

```

Finally, a few more administrative settings are configured on the Netscreen. Below, we disable the ability to reset a device for asset recovery. We also set the configuration file format storage type to unix, and disable the use of a system IP.

```
unset admin device-reset
set admin format unix
set admin sys-ip 0.0.0.0
```

The system IP option can be used to restrict access to the Netscreen device to a single configurable IP address. However, enabling this feature may cause confusion when troubleshooting firewall connectivity issues and there are simpler ways of achieving the same effects. Below we restrict management access from the security network, out of band network, and the Global Pro server; connection attempts from all other locations will fail.

```
set admin manager-ip 10.1.1.0 255.255.255.0
set admin manager-ip 4.4.4.4 255.255.255.255
```

Time Synchronization

To assist in troubleshooting and event correlation it is important to maintain consistent time across all systems and their corresponding log files. Whenever possible, NTP (network time protocol) should be enabled on network infrastructure devices. Below we configure the server IP address, timezone, and enable NTP operation.

```
set ntp timezone 0
set ntp server 10.1.1.6
set clock timezone 0
set clock ntp
```

If the system time is too far off, NTP will not synchronize properly. To keep this from happening, the 'set clock mm/dd/yyyy' command should be used to set the system clock to its initial value. The default NTP request interval of 10 minutes should be sufficient for most networks. Note that NTP MD5 authentication is not yet supported.

High Availability

In our network topology, if one Netscreen 500 were to fail, the redundant firewall would be there to pick up the slack by taking over all of the functions of the primary device. Here we have chosen to implement a simple HA configuration that does not involve load sharing across IP subnets. Though such a configuration is quite achievable with NSRP version 2, it does increase complexity and the number of interfaces required to distribute the load. Instead, if the additional bandwidth is not a high priority, it would be advisable to take the simpler approach of leaving the secondary device in a standby mode.

Once HA is enabled on both firewalls, the slave device will no longer be reachable through the same IP addresses. This is because the slave will

take on all the characteristics of the primary firewall including IPs. One must enable *different* management IP addresses on each of the firewalls in order to reach the slave device. This is configured like so:

```
MASTER  
set interface ethernet1/1 manage-ip 10.1.1.130  
set interface ethernet2/1 manage-ip 2.2.2.2
```

```
SLAVE  
set interface ethernet1/1 manage-ip 10.1.1.131  
set interface ethernet2/1 manage-ip 2.2.2.3
```

In order for the master and slave devices to communicate with each other, there must be an HA interface dedicated for HA traffic. This task is accomplished by placing an interface in the HA zone, and enabling HA on the interface.

```
set interface ethernet3/1 zone ha  
set ha interface ethernet3/1
```

Since HA communicates using a layer 2 protocol we do not need to configure an IP address for this interface. By default, HA is disabled on a Netscreen firewall. Changing the HA group from the default of 0 will automatically enable HA. Multiple groups can be configured for load sharing across multiple IP subnets. Here we use one group only.

```
set ha group 3
```

If two firewalls boot up simultaneously, the unit with the lowest MAC address will be selected as master during the HA election phase. To override this method of election, we configure different priorities on each device. The device with the lowest priority value is selected as master.

```
MASTER  
set ha priority 1
```

```
SLAVE  
set ha priority 10
```

To increase resilience, redundant Netscreen firewalls can be configured to poll specific locations as a measure of device reachability. Here we configure the Netscreen HA pair to poll the Internet router through ICMP echo-requests. If the no-response threshold is exceeded, a failover will be initiated to the slave device. The default poll interval and threshold have been changed from 1 to 10 seconds and from 255 to 3 respectively.

```
set ha track ip 2.2.2.254 interface Ethernet2/1  
set ha track ip 2.2.2.254 interval 10  
set ha track ip 2.2.2.254 threshold 3  
set ha method ping  
set ha track ip
```

By default, the interfaces on the slave device will remain in the downed state unless configured otherwise. The following command enables the links on slave device so that Spanning Tree won't slow down failover if it is enabled on the switch the firewall ports connect to.

```
set ha link-up-on-slave
```

By eliminating the election phase for pairs of Netscreens we can also improve the failover times. Election is only required for firewall HA groups of three or more devices.

```
set ha fast-mode
```

Though in our topology we use crossover cables to communicate between redundant firewalls, it is generally good practice to enable authentication and encryption of HA traffic. Encryption is much more important when using shared interfaces and a shared medium for inter-device communication.

```
set ha authentication password <password>
set ha encryption password <password>
```

Finally, configurations between master and slave can be quickly synchronized by issuing the 'exec ha file-sync' command. Keep in mind that any specific changes to the slave manage-ip settings are overwritten with this command and will need to be reconfigured.

VPN

Seven VPNs exist in our topology: six site-to-site and one dynamic. The site-to-site VPNs are quite straightforward. All traffic destined between the hub trust and security networks and the spoke networks is tunneled with no restrictions on services. A special VPN is configured to terminate at the Global Pro cloud. Only the global-pro service will be allowed to traverse this VPN.

An IKE gateway refers to IPSEC phase 1, while a VPN refers to IPSEC phase 2. Following are the IPSEC phase 1 and phase 2 configurations for the spoke and Global-Pro sites.

```
set ike gateway spokel ip 3.3.3.1 main preshare secret1 proposal pre-g2-3des-sha
set ike gateway spoke2 ip 3.3.3.5 main preshare secret2 proposal pre-g2-3des-sha
set ike gateway gp ip 5.5.5.5 main preshare secret3 proposal pre-g2-3des-sha
```

```
set vpn spokel gateway spokel no-replay tunnel proposal g2-esp-3des-md5
set vpn spoke2 gateway spoke2 no-replay tunnel proposal g2-esp-3des-md5
set vpn gp gateway gp no-replay tunnel proposal g2-esp-3des-md5
```

Notice that the IPSEC negotiations used for phase 1 and 2 have not been defined. This is because we have used one of the predefined negotiation settings that come standard on Netscreen devices. For IPSEC phase 1 we use a preshared key, Diffie-Hellman Group 2, 3DES encryption, with a SHA-1 hash. For IPSEC phase 2 we also use Diffie-Hellman Group 2, Encapsulating Security Protocol, 3DES encryption, and an MD5 hash.

It may be handy to store settings that can be used for VPNs terminating at a Check Point firewall. Below we create additional phase 1 and phase 2 negotiations for this purpose though they are not used in our topology.

```
set ike p1-proposal pre-g2-3des-sha-10080m preshare group2 esp 3des sha minute
10080
```

```
set ike p2-proposal g1-3des-md5-3600s group1 esp 3des md5 second 3600
```

Note that we are relying on default Check Point policy property settings for IKE and IPSEC. The above settings also assume PFS is selected for IPSEC phase 2 negotiations as Check Point uses DH group 1 for this purpose. If PFS is not desired, then a corresponding DH group 2 proposal should be used in its place.

The final step in creating a VPN is to enable a corresponding policy in the firewall rulebase. This is accomplished by creating an inbound and outbound rule on both ends of the VPN for bi-directional connectivity. Before configuring any policies we must remember to add all relevant network entries to our address book. Of special note is the naming convention used throughout this paper where addresses are preceded by a "H_" or "N_" to delineate hosts or networks. Additionally, network addresses are followed by a "-xx" designation to specify that number of bits in the network mask. A trailing "-24" represents a network with a 24 bit mask.

```
set address trust N_10.1.2.0-24 10.1.2.0 255.255.255.0 "Hub 1 LAN"
set address sec N_10.1.1.0-25 10.1.1.0 255.255.255.128 "Security Lan"
set address untrust N_10.1.3.0-24 10.1.3.0 255.255.255.0 "Spoke 1 LAN"
set address untrust N_10.1.4.0-24 10.1.4.0 255.255.255.0 "Spoke 2 LAN"
set address untrust H_4.4.4.4 4.4.4.4 255.255.255.255 "Global-Pro Server"
```

```
set policy from trust to untrust N_10.1.2.0-24 N_10.1.3.0-24 any tunnel vpn spoke1
set policy from untrust to trust N_10.1.3.0-24 N_10.1.2.0-24 any tunnel vpn spoke1
```

```
set policy from trust to untrust N_10.1.2.0-24 N_10.1.4.0-24 any tunnel vpn spoke2
set policy from untrust to trust N_10.1.4.0-24 N_10.1.2.0-24 any tunnel vpn spoke2
```

```
set policy from trust to untrust N_10.1.2.0-24 N_10.1.3.0-24 "NS Global Pro"
tunnel vpn gp
set policy from untrust to trust N_10.1.3.0-24 N_10.1.2.0-24 "NS Global Pro"
tunnel vpn gp
```

```
set policy from sec to untrust N_10.1.1.0-25 N_10.1.3.0-24 any tunnel vpn spoke1
set policy from untrust to sec N_10.1.3.0-24 N_10.1.1.0-25 any tunnel vpn spoke1
```

```
set policy from sec to untrust N_10.1.1.0-25 N_10.1.4.0-24 any tunnel vpn spoke2
set policy from untrust to sec N_10.1.4.0-24 N_10.1.1.0-25 any tunnel vpn spoke2
```

Optionally, the words "log" and "count" can be appended to the end of each policy for accounting and logging purposes, though we have not chosen to do so in this scenario.

For additional resilience, ScreenOS incorporates a proprietary protocol that enables IPSEC heartbeats to detect VPN tunnel failures. Though a more efficient and interoperable method of detecting tunnel failures has been developed in the Cisco Dead Peer Detection (DPD) draft [1], it has not yet been adopted in the Netscreen code. Of special note is that the draft has also expired as of January 2002 in its current state, though it has been implemented on the Cisco PIX and IOS.

Below, we set the hub site to probe both spoke gateways at specified 10 second intervals, with a retry threshold of 3. IPSEC will be forced to renegotiate phase 1 and phase 2 keys for the failed VPN if the retry threshold is exceeded.

```
set ike gateway spoke1 heartbeat hello 10
set ike gateway spoke1 heartbeat threshold 3
set ike gateway spoke2 heartbeat hello 10
set ike gateway spoke2 heartbeat threshold 3
```

The final VPN that must be configured is the one for remote dialup users. Since we cannot tie a static IP address to a remote gateway, we must choose some other form of authenticating these remote dynamic connections. In our case we chose an e-mail address and a shared key. Below we configure two remote IKE users named “client1” and “client2” using unique e-mail addresses. We also leave the share limit at the default of 1 so that multiple concurrent connections are not allowed.

```
set user client1 ike-id u-fqdn client1@site.com share-limit 1
set user client1 type ike
set user client1 enable
set user client2 ike-id u-fqdn client2@site.com share-limit 1
set user client2 type ike
set user client2 enable
```

By placing the usernames in a dialup group we can reference it more easily when creating an IKE gateway for IPSEC phase 1 negotiations.

```
set dialup ireclients + client1
set dialup ireclients + client2
```

The last step in configuring a dialup VPN is to create the corresponding ‘gateway’ and ‘vpn’ settings much like a standard site-to-site VPN. Below we reference our ‘remoteusers’ dialup group, set the preshared secret and IPSEC phase 1 negotiation parameters.

```
set ike gateway remoteusers dialup ireclients main preshare clientkey proposal
pre-g2-3des-sha
```

A handy setting to enable is nat-traversal which is used to encapsulate ESP packets in UDP packets to allow transmission of encrypted traffic through a NAT device.

```
set ike gateway remoteusers nat-traversal udp-checksum
set ike gateway remoteusers nat-traversal keepalive-frequency 5
```

Next, the VPN statement references the IKE gateway we just created.

```
set vpn remoteusers gateway remoteusers no-replay tunnel proposal g2-esp-3des-md5
```

Lastly, to allow inbound remote dialup VPN connections a policy must be added to the existing hub rulebase.

```
set policy from untrust to trust "Dial-Up VPN" N_10.1.2.0-24 any tunnel vpn-dialup
remoteusers count log
```

At this point, remote users should be able to connect to the hub site assuming they have properly configured their Netscreen IRE Client settings. It may be advisable to limit the ports over which they are allowed to enter, though we have not chosen to do so here.

Following, are a few additional settings related to VPNs that are part of our standard template. Below we have chosen to limit the number of responses to bad a spi after a Netscreen reboot to only one. We have also enable subnet negotiation for IKE allowing for finer granularity when bringing up IPSEC tunnels.

```
set ike respond-bad-spi 1
set ike id-mode subnet
```

Finally, we remove the IPSEC phase 1 policy matching requirement and the ability to match proposals outside the ones explicitly referenced in the 'gateway' and 'vpn' settings.

```
unset ike policy-checking
unset ike accept-all-proposal
```

Policies

Policies have already been configured to allow VPN tunnels to function properly. However, additional services are required in our topology including access to the servers in the DMZ LAN, access from the DMZ to the Trusted LAN, and access from the Secure and Trusted LANs to the Internet. For the sake of brevity this section does not presume to add all the policies required that would be necessary in a live environment. Rather, policies are added to give the reader a flavor for what might be necessary in a production rulebase.

All inter-zone traffic will be blocked by default unless explicitly allowed through a firewall policy.

```
set zone untrust block
set zone dmz block
set zone mgt block
set zone trust block
set zone sec block
```

Outbound NTP will be allowed from the NTP server to the Internet so it can synchronize with a stratum 2 source. This traffic will be subject to NAT as if it is coming from the external interface of the firewall itself.

```
set address sec H_10.1.1.6 10.1.1.6 255.255.255.255 "Utility Server"
set policy from sec to untrust H_10.1.1.6 out-any ntp nat permit
```

NTP and syslog traffic will be allowed from the hub networks to the utility server.

```
set address dmz H_10.1.0.5 10.1.0.5 255.255.255.255 "DNS Server"
set address dmz H_10.1.0.6 10.1.0.6 255.255.255.255 "Web Server"
set address dmz N_10.1.0.0-24 10.1.0.0 255.255.255.0 "DMZ Lan"

set address trust H_10.1.2.5 10.1.2.5 255.255.255.255 "DB1 Server"
set address trust H_10.1.2.6 10.1.2.6 255.255.255.255 "DB2 Server"
set address trust N_10.1.2.0-24 10.1.2.0 255.255.255.0 "Trust Lan"

set group service utility add ntp
set group service utility add syslog

set policy from dmz to sec N_10.1.0.0-24 H_10.1.1.6 utility permit
set policy from trust to sec N_10.1.2.0-24 H_10.1.1.6 utility permit
```

Additionally, RADIUS authentication requests from the hub site will be forwarded to the AAA server. RADIUS is not a predefined service, so we must define it ourselves.

```
set service radius protocol udp src-port 1024-65535 dst-port 1812-1812
set address sec H_10.1.1.5 10.1.1.5 255.255.255.255 "AAA Server"
set policy from dmz to sec N_10.1.0.0-24 H_10.1.1.5 radius permit
set policy from trust to sec N_10.1.2.0-24 H_10.1.1.5 radius permit
```

The Web server in the DMZ communicates with the database servers through a special TCP port only. Once again we must configure the service before referencing it in a policy.

```
set service dbapp protocol tcp src-port 1024-65535 dst-port 9900-9900
set address trust N_10.1.2.5-31 10.1.2.5 255.255.255.254 "DB Servers"

set policy from dmz to trust H_10.1.0.6 N_10.1.2.5-31 dbapp permit
```

Inbound web and DNS should be permitted to the servers in the DMZ. A MIP (mapped IP) is used in this instance to create a static mapping between the public and private IP address for each server.

```
set interface untrust mip 2.2.2.5 host 10.1.0.5 netmask 255.255.255.255
set interface untrust mip 2.2.2.6 host 10.1.0.6 netmask 255.255.255.255

set group service web add http
set group service web add https

set policy from untrust to dmz out-any H_10.1.0.5 dns permit
set policy from untrust to dmz out-any H_10.1.0.6 web permit
```

In order for the DNS server to perform DNS services for internal hosts, it should be allowed to issue DNS queries to the Internet.

```
set policy from dmz to untrust H_10.1.0.5 out-any dns permit
```

To assist in troubleshooting and to improve overall network resilience, we define a safe subset of the ICMP protocol [2] in individual services and allow them globally. ScreenOS unfortunately makes it a bit difficult to define ICMP codes but not entirely impossible. An easy way to understand how to specify an ICMP type and code is to first be aware that the offset of the source port in a TCP or UDP packet is the exact same offset and length as the ICMP type and code. For example, if you take the predefined ping service and convert the source-port information (2048) into HEX (0800), you will have the ICMP type 8 code 0 which is an ICMP echo-request! Following that same logic, we map services for ICMP_ECHO, ICMP_UNREACH, ICMP_SOURCEQUENCH, and ICMP_TIMXCEED, in that order.

```
set service icmp-safe protocol 1 src-port 2048-2048 dst-port 0-65535
set service icmp-safe + 1 src-port 768-789 dst-port 0-65535
set service icmp-safe + 1 src-port 1024-1024 dst-port 0-65535
set service icmp-safe + 1 src-port 4352-4353 dst-port 0-65535
```

```
set address mgt N_10.1.1.128-25 10.1.1.128 255.255.255.128 "Mgt Lan"
```

```
set policy from trust to untrust N_10.1.2.0-24 out-any icmp-safe permit
set policy from trust to sec N_10.1.2.0-24 N_10.1.1.0-25 icmp-safe permit
set policy from sec to trust N_10.1.1.0-25 N_10.1.2.0-24 icmp-safe permit
set policy from trust to dmz N_10.1.2.0-24 N_10.1.0.0-24 icmp-safe permit
set policy from dmz to trust N_10.1.0.0-24 N_10.1.2.0-24 icmp-safe permit
set policy from dmz to untrust N_10.1.0.0-24 out-any icmp-safe permit
```

```
set policy from untrust to dmz out-any N_10.1.0.0-24 icmp-safe permit
set policy from sec to untrust N_10.1.1.0-25 out-any icmp-safe permit
```

Keep in mind that in ScreenOS ICMP is stateful, so policies and services for ICMP echo-replies do not need to be configured.

Inbound ICMP traffic from the Internet is a prime candidate for rate limiting. This can be accomplished at the border routers, or on the firewalls themselves. We have chosen to leave inbound rate-limiting at the border routers because it is farther upstream, though doing so on the Netscreen itself would be quite simple indeed.

Traffic Screening

In addition to policy filtering, advanced firewalls can also provide protection by watching for specific attack signatures or illegal traffic patterns. Perhaps one of the most common signatures is the TCP SYN flood. ScreenOS comes with a feature named TCP Proxy designed to protect hosts from TCP SYN floods.

TCP Proxy relies on well defined parameters from which to operate. SYN flood protection parameters should generally be based on network size and the amount of traffic that is expected per host. By watching the amount of TCP SYN traffic to each internal IP and port tuple, the firewall is able to act as a TCP handshake mediator in times of stress.

Special care should be taken to tune these parameters to individual network requirements. Below we have configured TCP Proxy to begin generating alarms at 1000 half-complete pps and to start proxying at 1500 pps. The firewall will hold up to 10,000 packets in the pending queue before rejecting new connections allowing half-open connections to remain in the queue for up to 10 seconds. A maximum of 250 pending connections will be allowed from a single source IP address.

```
set interface ethernet2/1 screen syn-flood alarm-threshold 1000
set interface ethernet2/1 screen syn-flood attack-threshold 1500
set interface ethernet2/1 screen syn-flood source-threshold 250
set interface ethernet2/1 screen syn-flood queue-size 10000
set interface ethernet2/1 screen syn-flood timeout 10
```

Other special firewall screening settings that require fine tuning based on network size and individual requirements are listed below. The ip-sweep threshold is measured in microseconds, port-scan in milliseconds, and all other settings in packets per second.

```
set interface ethernet2/1 screen ip-sweep
set interface ethernet2/1 screen ip-sweep threshold 1000
set interface ethernet2/1 screen port-scan
set interface ethernet2/1 screen icmp-flood
set interface ethernet2/1 screen icmp-flood threshold 100
set interface ethernet2/1 screen udp-flood
set interface ethernet2/1 screen udp-flood threshold 1000
set interface ethernet2/1 screen limit-session source-ip-based 4096
```

A nice way of filtering malicious web queries is to use the mal-url directive. The code-red worm is a predefined directive which we reference below. Note that URL matching must occur from the beginning of an HTTP GET request, so mid-URL pattern matching for nimda [3] using “/cmd.exe?” will not work.

```
set interface ethernet2/1 screen mal-url code-red
```

The following attack types should be filtered at the network edge excluding the component-block setting which allows for JAVA and ActiveX components to flow uninhibited.

```
unset interface ethernet2/1 screen component-block
set interface ethernet2/1 screen icmp-fragment
set interface ethernet2/1 screen icmp-large
set interface ethernet2/1 screen fin-no-ack
set interface ethernet2/1 screen ip-bad-option
set interface ethernet2/1 screen ip-filter-src
set interface ethernet2/1 screen ip-loose-src-route
set interface ethernet2/1 screen ip-strict-src-route
set interface ethernet2/1 screen ip-record-route
set interface ethernet2/1 screen tear-drop
set interface ethernet2/1 screen winnuke
set interface ethernet2/1 screen ip-spoofing
set interface ethernet2/1 screen ping-death
set interface ethernet2/1 screen land
set interface ethernet2/1 screen ip-security-opt
set interface ethernet2/1 screen ip-stream-opt
set interface ethernet2/1 screen syn-frag
set interface ethernet2/1 screen syn-fin
set interface ethernet2/1 screen tcp-no-flag
set interface ethernet2/1 screen unknown-protocol
set interface ethernet2/1 screen ip-timestamp-opt
```

IP spoofing should not be allowed on any interfaces, so it should be configured on every interface of the firewall. It is expected that other attack types should not generally be seen on the internal hub network, though the above settings can be replicated to any interface of the firewall in addition to the untrusted.

```
set interface ethernet1/1 screen ip-spoofing
set interface ethernet1/2 screen ip-spoofing
set interface ethernet2/1 screen ip-spoofing
set interface ethernet2/2 screen ip-spoofing
```

To protect the session table from being flooded with non-first TCP packets such as TCP ACKs, the firewall should be configured to disallow TCP traffic that has not been properly initiated with the three-way handshake. Check Point firewalls have had this feature enabled by default since version 4.1. Netscreen firewalls do not enable this feature by default in the event that a network is performing asynchronous routing, and the firewall does not always see the entire TCP traffic flow.

```
set flow tcp-syn-check
set flow tcp-syn-check-in-tunnel
```

Finally, some additional flow settings should be enabled to improve network performance and resilience as follows:

```
set flow tcp-mss
set flow mac-flooding
```

```
set flow check-session
set flow path-mtu
set flow init 20
```

Miscellaneous

For the settings that don't necessarily fit in any other category we reserve the infamous miscellaneous category. However, do not let the title diminish the importance of the configuration statements to follow. In HA environments it is crucial that MAC learning be disabled for source frames as many strange flow-related problems are likely to occur if this is not done. This flag is especially necessary in networks that incorporate forms of high availability such as VRRP and HSRP where frames do not always arrive with the same source MAC address.

```
set arp always-on-dest
```

Last but not least, we list the static routes necessary to route all traffic from the trust-vr, out to the untrust-vr, and then to the upstream gateway.

```
set vrouter trust-vr route 0.0.0.0/0 vrouter untrust-vr
set vrouter untrust-vr route 0.0.0.0/0 interface untrust gateway 2.2.2.254
```

Conclusion

One concept that we often forget is that firewalls are designed to **enhance NOT replace** additional measures of network security. A single open service allowed by the firewall could be the death of a server behind if it is not properly protected and updated at the host level. Though the focus of this paper surrounds firewall configurations, the importance of additional regular measures of network and server security cannot be stressed enough.

A complete list of ScreenOS configuration guidelines were presented in this document to assist security administrators in hardening their Netscreen firewalls. As one of the major links in the funneled approach to network security, firewalls provide a highly granular toolkit with which to filter unwanted traffic. This document should serve as a reference for readers who wish to audit and standardize their Netscreen firewall configurations based on current industry best practices.

References

[1] G. Huang, S. Beaulieu, D. Rochefort, "A Traffic-Based Method of Detecting Dead IKE Peers", July 2001.

<http://www.ietf.org/proceedings/01dec/I-D/draft-ietf-ipsec-dpd-00.txt>

[2] Thomas, Rob, "ICMP Packet Filtering", February 2002.

<http://www.cymru.com/Documents/icmp-messages.html>

[3] CERT, "CERT Advisory CA-2001-26 Nimda Worm", September 2001.

Appendix A

Following is the entire configuration presented in this document for the master hub Netscreen 500 without descriptions or annotations. We leave it as an exercise for the reader to create the appropriate configurations for the slave Netscreen and the firewalls at each of the spoke sites.

```
set syslog config 10.1.1.6 local0 local0 notice
set syslog enable
set syslog traffic
set firewall log-self
set firewall log-self ike
set firewall log-self snmp
set admin mail server-name 10.1.1.6
set admin mail mail-addr1 gillsr@yahoo.com
set admin mail traffic-log
set interface mgt ip 10.1.1.129/25
set interface mgt manage ping
set interface mgt manage scs
unset interface mgt manage telnet
set interface mgt manage snmp
unset interface mgt manage global
set interface mgt manage global-pro
set interface mgt manage ssl
set interface mgt manage web
set interface ethernet1/1 zone trust
set interface ethernet1/1 ip 10.1.2.1/24
set interface ethernet1/1 route
set interface ethernet1/1 manage ping
set interface ethernet1/1 manage scs
unset interface ethernet1/1 manage telnet
unset interface ethernet1/1 manage snmp
unset interface ethernet1/1 manage global
set interface ethernet1/1 manage global-pro
unset interface ethernet1/1 manage ssl
unset interface ethernet1/1 manage web
unset interface ethernet1/1 ident-reset
set zone name sec
set zone sec vrouter trust-vr
set interface ethernet1/2 zone sec
set interface ethernet1/2 ip 10.1.1.1/25
set interface ethernet1/2 route
set interface ethernet1/2 manage ping
set interface ethernet1/2 manage scs
unset interface ethernet1/2 manage telnet
unset interface ethernet1/2 manage snmp
unset interface ethernet1/2 manage global
set interface ethernet1/2 manage global-pro
unset interface ethernet1/2 manage ssl
unset interface ethernet1/2 manage web
unset interface ethernet1/2 ident-reset
set scs enable
set snmp community sh0wm3th3$ Read-Only Trap-on
set snmp host sh0wm3th3$ 10.1.1.6
set snmp contact "Stephen Gill"
set snmp location "Test Lab"
set snmp name "NS500"
set hostname ns500
set domain site.com
set global-pro enable
set global-pro vpn
set global-pro config primary 4.4.4.4
set global-pro policy-manager primary host 4.4.4.4
set global-pro report proto-dist enable
set global-pro report ethernet-stat enable
set global-pro report attack-stat enable
set global-pro report flow-stat enable
set global-pro report policy-stat enable
set global-pro report alarm-traffic enable
set global-pro report alarm-attack enable
set global-pro report alarm-other enable
```

```

set global-pro report log-config enable
set global-pro report log-info enable
set global-pro report log-self enable
set global-pro report log-traffic enable
set interface ethernet2/1 zone untrust
set interface ethernet2/1 ip 2.2.2.1/24
set interface ethernet2/1 manage ping
unset interface ethernet2/1 manage scs
unset interface ethernet2/1 manage telnet
unset interface ethernet2/1 manage snmp
unset interface ethernet2/1 manage global
unset interface ethernet2/1 manage global-pro
unset interface ethernet2/1 manage ssl
unset interface ethernet2/1 manage web
unset interface ethernet2/1 ident-reset
set interface ethernet2/2 zone dmz
set zone dmz vrouter untrust-vr
set interface ethernet2/2 ip 10.1.0.1/24
set interface ethernet2/2 manage ping
unset interface ethernet2/2 manage scs
unset interface ethernet2/2 manage telnet
unset interface ethernet2/2 manage snmp
unset interface ethernet2/2 manage global
unset interface ethernet2/2 manage global-pro
unset interface ethernet2/2 manage ssl
unset interface ethernet2/2 manage web
unset interface ethernet2/2 ident-reset
set auth type 1
set auth server-name 10.1.1.5
set auth secret <secret>
set auth radius-port 1812
set auth timeout 10
unset admin device-reset
set admin name "admin"
set admin password nEbYCyrbAZGKcQHHDsEAioItl1DIIn
set admin auth type radius
set admin auth server-name 10.1.1.5
set admin auth secret <secret>
set admin auth radius-port 1812
set admin auth timeout 10
set admin format unix
set admin sys-ip 0.0.0.0
set admin manager-ip 10.1.1.0 255.255.255.0
set admin manager-ip 4.4.4.4 255.255.255.255
set ntp timezone 0
set ntp server 10.1.1.6
set clock timezone 0
set clock ntp
set interface ethernet1/1 manage-ip 10.1.1.130
set interface ethernet2/1 manage-ip 2.2.2.2
set interface ethernet3/1 zone ha
set ha interface ethernet3/1
set ha group 3
set ha priority 1
set ha track ip 2.2.2.254 interface Ethernet2/1
set ha track ip 2.2.2.254 interval 10
set ha track ip 2.2.2.254 threshold 3
set ha method ping
set ha track ip
set ha link-up-on-slave
set ha fast-mode
set ha authentication password <password>
set ha encryption password <password>
set ike gateway spoke1 ip 3.3.3.1 main preshare secret1 proposal pre-g2-3des-sha
set ike gateway spoke2 ip 3.3.3.5 main preshare secret2 proposal pre-g2-3des-sha
set vpn spoke1 gateway spoke1 no-replay tunnel proposal g2-esp-3des-md5
set vpn spoke2 gateway spoke1 no-replay tunnel proposal g2-esp-3des-md5
set ike p1-proposal pre-g2-3des-sha-10080m preshare group2 esp 3des sha minute
10080
set ike p2-proposal g1-3des-md5-3600s group1 esp 3des md5 second 3600
set ike gateway spoke1 heartbeat hello 10
set ike gateway spoke1 heartbeat threshold 3
set ike gateway spoke2 heartbeat hello 10
set ike gateway spoke2 heartbeat threshold 3
set user client1 ike-id u-fqdn client1@site.com share-limit 1
set user client1 type ike
set user client1 enable
set user client2 ike-id u-fqdn client2@site.com share-limit 1
set user client2 type ike
set user client2 enable
set dialup ireclients + client1

```

```

set dialup ireclients + client2
set ike gateway remoteusers dialup ireclients main preshare clientkey proposal
pre-g2-3des-sha
set ike gateway remoteusers nat-traversal udp-checksum
set ike gateway remoteusers nat-traversal keepalive-frequency 5
set vpn remoteusers gateway remoteusers no-replay tunnel proposal g2-esp-3des-md5
set policy from untrust to trust "Dial-Up VPN" N_10.1.2.0-24 any tunnel vpn-dialup
remoteusers count log
set ike respond-bad-spi 1
set ike id-mode subnet
unset ike policy-checking
unset ike accept-all-proposal
set zone untrust block
set zone dmz block
set zone mgt block
set zone trust block
set zone sec block
set address sec H_10.1.1.5 10.1.1.5 255.255.255.255 "AAA Server"
set address sec H_10.1.1.6 10.1.1.6 255.255.255.255 "Utility Server"
set address sec N_10.1.1.0-25 10.1.1.0 255.255.255.128 "Security Lan"
set address dmz H_10.1.0.5 10.1.0.5 255.255.255.255 "DNS Server"
set address dmz H_10.1.0.6 10.1.0.6 255.255.255.255 "Web Server"
set address dmz N_10.1.0.0-24 10.1.0.0 255.255.255.0 "DMZ Lan"
set address trust H_10.1.2.5 10.1.2.5 255.255.255.255 "DB1 Server"
set address trust H_10.1.2.6 10.1.2.6 255.255.255.255 "DB2 Server"
set address trust N_10.1.2.0-24 10.1.2.0 255.255.255.0 "Trust Lan"
set address trust N_10.1.2.0-24 10.1.2.0 255.255.255.0 "Hub 1 LAN"
set address trust N_10.1.2.5-31 10.1.2.5 255.255.255.254 "DB Servers"
set address untrust N_10.1.3.0-24 10.1.3.0 255.255.255.0 "Spoke 1 LAN"
set address untrust N_10.1.4.0-24 10.1.4.0 255.255.255.0 "Spoke 2 LAN"
set address untrust H_4.4.4.4 4.4.4.4 255.255.255.255 "Global-Pro Server"
set address mgt N_10.1.1.128-25 10.1.1.128 255.255.255.128 "Mgt Lan"
set group service utility add ntp
set group service utility add syslog
set group service web add http
set group service web add https
set service radius protocol udp src-port 1024-65535 dst-port 1812-1812
set service dbapp protocol tcp src-port 1024-65535 dst-port 9900-9900
set service icmp-safe protocol 1 src-port 2048-2048 dst-port 0-65535
set service icmp-safe + 1 src-port 768-789 dst-port 0-65535
set service icmp-safe + 1 src-port 1024-1024 dst-port 0-65535
set service icmp-safe + 1 src-port 4352-4353 dst-port 0-65535
set policy from trust to untrust N_10.1.2.0-24 N_10.1.3.0-24 any tunnel vpn spokel
set policy from trust to untrust N_10.1.2.0-24 N_10.1.4.0-24 any tunnel vpn spoke2
set policy from trust to untrust N_10.1.2.0-24 N_10.1.3.0-24 "NS Global Pro"
tunnel vpn gp
set policy from trust to untrust N_10.1.2.0-24 out-any icmp-safe permit
set policy from trust to sec N_10.1.2.0-24 H_10.1.1.6 utility permit
set policy from trust to sec N_10.1.2.0-24 H_10.1.1.5 radius permit
set policy from trust to sec N_10.1.2.0-24 N_10.1.1.0-25 icmp-safe permit
set policy from trust to dmz N_10.1.2.0-24 N_10.1.0.0-24 icmp-safe permit
set policy from untrust to trust N_10.1.3.0-24 N_10.1.2.0-24 any tunnel vpn spokel
set policy from untrust to trust N_10.1.4.0-24 N_10.1.2.0-24 any tunnel vpn spoke2
set policy from untrust to trust N_10.1.3.0-24 N_10.1.2.0-24 "NS Global Pro"
tunnel vpn gp
set policy from untrust to dmz out-any H_10.1.0.5 dns permit
set policy from untrust to dmz out-any H_10.1.0.6 web permit
set policy from untrust to dmz out-any N_10.1.0.0-24 icmp-safe permit
set policy from untrust to sec N_10.1.3.0-24 N_10.1.1.0-25 any tunnel vpn spokel
set policy from untrust to sec N_10.1.4.0-24 N_10.1.1.0-25 any tunnel vpn spoke2
set policy from sec to untrust N_10.1.1.0-25 N_10.1.3.0-24 any tunnel vpn spokel
set policy from sec to untrust N_10.1.1.0-25 N_10.1.4.0-24 any tunnel vpn spoke2
set policy from sec to untrust H_10.1.1.6 out-any ntp nat permit
set policy from sec to untrust N_10.1.1.0-25 out-any icmp-safe permit
set policy from sec to trust N_10.1.1.0-25 N_10.1.2.0-24 icmp-safe permit
set policy from dmz to sec N_10.1.0.0-24 H_10.1.1.6 utility permit
set policy from dmz to sec N_10.1.0.0-24 H_10.1.1.5 radius permit
set policy from dmz to untrust H_10.1.0.5 out-any dns permit
set policy from dmz to untrust N_10.1.0.0-24 out-any icmp-safe permit
set policy from dmz to trust H_10.1.0.6 N_10.1.2.5-31 dbapp permit
set policy from dmz to trust N_10.1.0.0-24 N_10.1.2.0-24 icmp-safe permit
set interface untrust mip 2.2.2.5 host 10.1.0.5 netmask 255.255.255.255
set interface untrust mip 2.2.2.6 host 10.1.0.6 netmask 255.255.255.255
set interface ethernet2/1 screen syn-flood alarm-threshold 1000
set interface ethernet2/1 screen syn-flood attack-threshold 1500
set interface ethernet2/1 screen syn-flood source-threshold 250
set interface ethernet2/1 screen syn-flood queue-size 10000
set interface ethernet2/1 screen syn-flood timeout 10
set interface ethernet2/1 screen ip-sweep
set interface ethernet2/1 screen ip-sweep threshold 1000
set interface ethernet2/1 screen port-scan

```

```

set interface ethernet2/1 screen icmp-flood
set interface ethernet2/1 screen icmp-flood threshold 100
set interface ethernet2/1 screen udp-flood
set interface ethernet2/1 screen udp-flood threshold 1000
set interface ethernet2/1 screen limit-session source-ip-based 4096
set interface ethernet2/1 screen mal-url code-red
set interface ethernet2/1 screen mal-url nimda "/cmd.exe?/" 0
unset interface ethernet2/1 screen component-block
set interface ethernet2/1 screen icmp-fragment
set interface ethernet2/1 screen icmp-large
set interface ethernet2/1 screen fin-no-ack
set interface ethernet2/1 screen ip-bad-option
set interface ethernet2/1 screen ip-filter-src
set interface ethernet2/1 screen ip-loose-src-route
set interface ethernet2/1 screen ip-strict-src-route
set interface ethernet2/1 screen ip-record-route
set interface ethernet2/1 screen tear-drop
set interface ethernet2/1 screen winnuke
set interface ethernet2/1 screen ip-spoofing
set interface ethernet2/1 screen ping-death
set interface ethernet2/1 screen land
set interface ethernet2/1 screen ip-security-opt
set interface ethernet2/1 screen ip-stream-opt
set interface ethernet2/1 screen syn-frag
set interface ethernet2/1 screen syn-fin
set interface ethernet2/1 screen tcp-no-flag
set interface ethernet2/1 screen unknown-protocol
set interface ethernet2/1 screen ip-timestamp-opt
set interface ethernet1/1 screen ip-spoofing
set interface ethernet1/2 screen ip-spoofing
set interface ethernet2/1 screen ip-spoofing
set interface ethernet2/2 screen ip-spoofing
set flow tcp-syn-check
set flow tcp-syn-check-in-tunnel
set flow tcp-mss
set flow mac-flooding
set flow check-session
set flow path-mtu
set arp always-on-dest
set vrouter trust-vr route 0.0.0.0/0 vrouter untrust-vr
set vrouter untrust-vr route 0.0.0.0/0 interface untrust gateway 2.2.2.25

```