SANS Institute
InfoSec Reading Room

How To Implement Security in the MAX TNT RAS Server

This document intends to show the necessary configurations and cares to provide a more secure DIAL or ISDN (Integrated Service Digital Network) access network, based on equipments Lucent MAX TNT. Pointing the best practices, special configurations in the RAS Servers (Remote Access Service) and in the RADIUS (Remote Authentication Dial-In User Service) and management servers.

How To Implement Security in the *MAX TNT* RAS Server

Objective: This document intends to show the necessary configurations and cares to provide a more secure DIAL or ISDN (Integrated Service Digital Network) access network, based on equipments Lucent MAX TNT.
Pointing the best practices, special configurations in the RAS Servers (Remote Access Service) and in the RADIUS (Remote Authentication Dial-In User Service) and management servers.

Network Overview: Generally the main components of a network based on MAX TNT RAS servers are : the RAS Servers, Authentication, Authorization, Accounting and Management servers, as showed below.
This kind of access network can provide different services like DIAL-UP access, ISDN access, tunneling access with L2TP (Layer 2 Tunneling Protocol), PPTP (Point-to-Point Tunneling Protocol) and others.
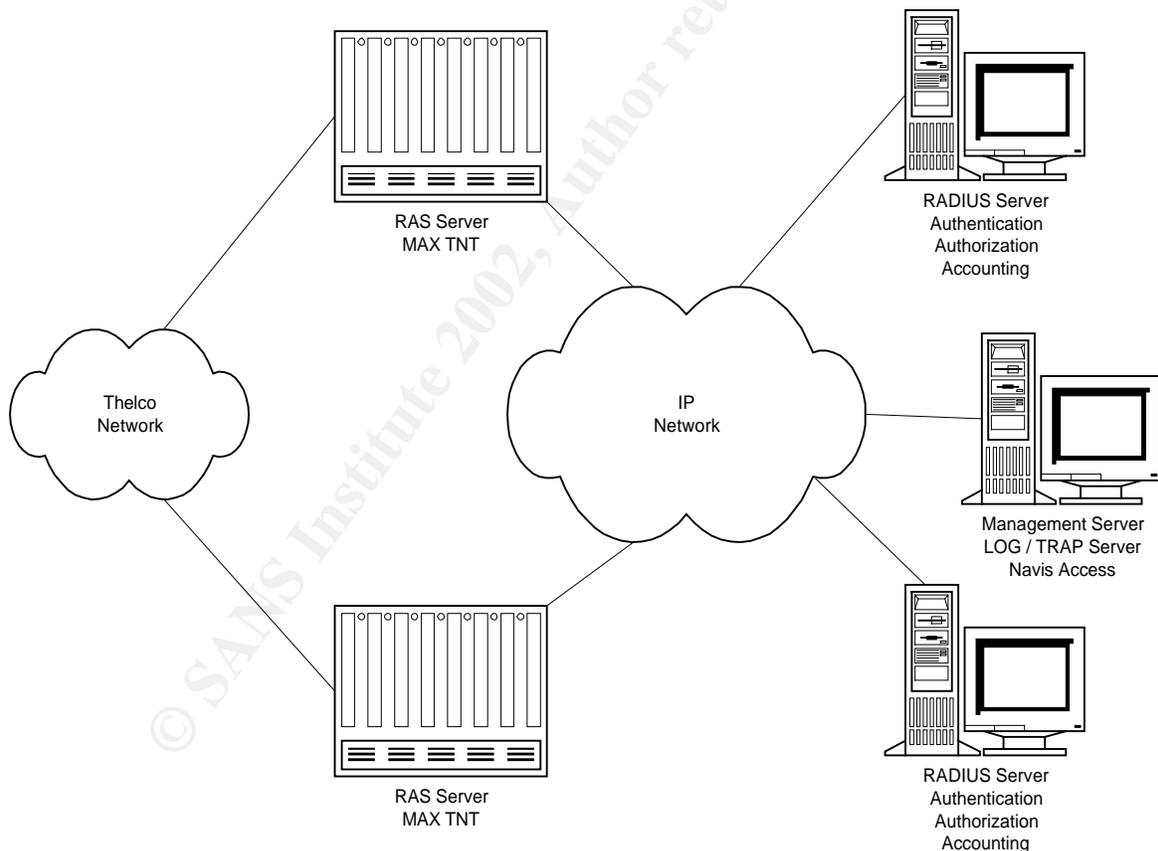
In this way it is not enough to secure the RAS Server, because it can't work alone, the other components should be secured too, then we need to take care about the security of the operational system and applications of all the related servers. This isn't the focus of this document although it is important to

remember that it can be a good idea to use a Firewall to protect these servers and to apply the best security practices for each server and applications.

The RADIUS is a protocol defined in the IETF RFC 2058 and 2059, and it can make the authentication, authorization and accounting. It has a user database, and it's possible to specify other attributes, like routing and filtering for each user. The RADIUS is an UDP based protocol and uses two ports : one for authentication and other for accounting, the default ports are 1645 and 1646 at the oldest versions and 1812 and 1813 at the newest versions respectively, but it is important to remeber that these ports number can be configured in the RADIUS servers and in the MAX TNT too.

Equipment: The MAX TNT server, is a modular equipment, then it can be composed with different hardware configurations. The examples shown in this document are based in a RAS server with the hardware configuration shown as follow, which can provide 480 simultaneous RAS connections and more 480 simultaneous ISDN connections.

- 04 serial interfaces, composing the in and outbound backbone
- 04 ethernet interfaces, used, in our case, for management
- 04 E1 cards, with 8 E1's ports each
- 10 modem cards with 48 modems each

The MAX TNT software is proprietary and has a CLI (Command Line Interface) and is called TAOS (True Access Operating System). All the examples shown in this document are based on the 9.0.0 version of the TAOS, but most of them are compatible with older versions too.

The TAOS is based on profiles, and each profile has the purpose to configure a set of features, like SNMP Profile, USER profile and so on.
A group of commands are global, like READ, WRITE, ADD, LIST, SET, GET and others. These commands are used to set the features to the suitable values.

Default Settings: The equipment comes from the factory, with default settings, like : the access to the equipment with the *Admin* user and password *Ascend*.
These default settings can cause, if we do not observe them, big future problems. Some of them are related with security, like default passwords and SNMP (Simple Network Management Protocol) string communities. More complex examples can refer to weak points of the equipment like access over an E1 connection through a terminal server.

Best Practices and Security Configurations
for the MAX TNT RAS Servers

Equipment Access, Users and Passwords: The MAX TNT Server supports a TELNET access and the default user is *Admin* with the password *Ascend*. Unfortunately the equipment doesn't support access through cryptographed protocols like the SSH (Secure Shell).
In this case the advices are :

- change periodically all the access passwords to the equipment based on a previous defined security policy
- remove the administrator privileges from the Admin account and change its password
- choose biggest passwords with different kind of characters, because in the TELNET access the information will travel in clear text in the network
- avoid the access to the equipments through non-reliable networks, or better through unknown networks
- create a new account with the administrator privileges with a non-sugestive noun
- create individual accounts for every user that needs access to the equipment with the right privilegies
- configure all the users so that they can't view the other passwords, because in the default configuration, every user can read and list the other passwords, being possible to impersonate them
- specify the idle time for the sessions to avoid forgotten consoles opened and attacks based on Denial of Service of Sessions.
- enable the TELNET password which is required before the user and password validation.

The following commands configure the access to the equipment :

```
read ip-global
 set telnet-password = <password>   // change a telnet password
 write

read system
 set idle-logout = 10               // specify the idle-timer
 read user admin
 set password = <password>          // change this user password
 set idle-logout = 10               // specify a 10-minute idle timer
 set allow-password = no            // disable this user to view the passwords
 set system = no                    // disable the write rights
 write
```

```
new user <new-administrator>      // create a new administrator
 set active-enabled = yes         // enable this user
 set password = <password>
 set idle-logout = 10
 set allow-password = no
 set system = yes                 // enable the write rights
 write
```

The *auth* command can be used to change the user privilegies in an established session, similar to the *su* UNIX command.


Clock Synchronism: The clock synchronism of the equipments is extremely important, because only in this case we will can efficiently trace the connections and disconnections time. Also the RADIUS server shall be synchronyzed through a NTP (Network Time Protocol) Server, because they store all the user accounting and information. Another important point of the synchronism is the failure correlation provided by the management system. In the default configuration the clock synchronism is disabled, the clock base is local and the timezone is zero. The following commands configure the NTP in the MAX TNT:

```
read ip-global
 list sntp-info
 set gmt-offset = <off-set>                   // specify a timezone like -0300
 set host 1 = <IP-Address-NTP-Server-1>       // Primary NTP Server
 set host 2 = <IP-Address-NTP-Server-2>       // Secondary NTP Server
 set enabled = sntp-enabled
 write
```

4

The commands **sntp –d** and **date** can be used to verify the NTP status and the current date and time respectively.
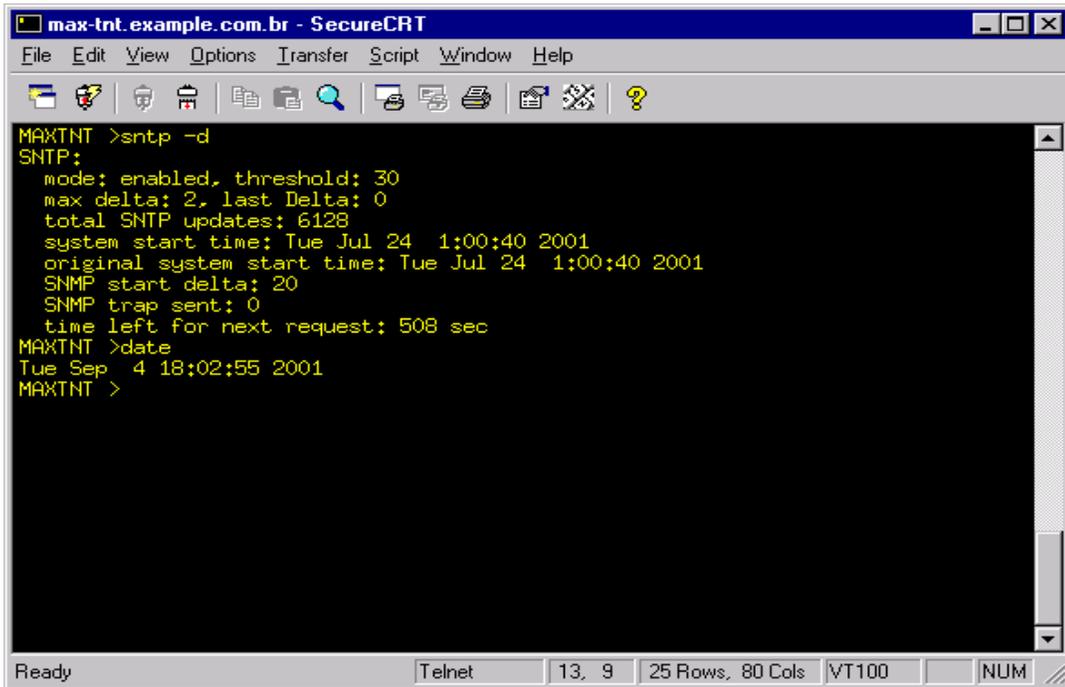
Non Essential Services: To avoid violations through the non-essential services, provided in the default configuration, it is strongly recommended to analyze, remove or disable them.

The following commands disable some of the non-essential services :

read ip-global
set finger =no   *// disable the FINGER service*
set user-profile = ""   *// disable the automatic send of the*
write   *// profile in the TELNET connections*

The *finger* service is not necessary in most cases, and it can represent a weak security point because through it an attacker can discover the users created in the equipment.

The *user-profile* is the default user used in a telnet session, then it's interesting to set it as null, forcing typing the user name. In some versions of TAOS the default is null but in other versions it can be Admin.

Log : It's pretty necessary the extraction of the log registers from the equipments. Not only for security purposes but to analyze traffic and failures too.

In this way it's interesting to configure the MAX TNT to send the logs to a centralized syslog server, especially, because there is an internal buffer in the MAX TNT to store the logs but it is not enough to keep a log for a suitable period of time and in case of a reboot in the equipment the log would be lost.

The following commands should be applied :

```
   read log
    set syslog-enable = yes          // enable the general log
    set call-info = end-of-call      // logs at the end of the call
    set host = <Syslog-Server-IP>    // specify the general syslog server
    set save-level = debug           // especify the log level
    write

   read call-logging
    set call-log-enable = yes             // enable the call log
    set call-log-host-1 = <IP-Syslog-Server>   // specify the syslog for calls
    set call-log-key= <Secret-Key>        // specify the  secret-key
    set call-log-timeout = 20
    write
```

To allow that the RADIUS server stores the number of the calling station, or better, the source of a call, it is necessary that each E1 has the correct configuration in the switch-type. Its is important to remember that storing the calling station number is essential for security purposes, because we can identify, based on logs, the user used in any connection. But the users and passwords can be stolen and in this case the calling station number is the way to identify the user, because it's much more difficult to spoof this number.

The following commands should be applied in each E1 :

```
   read e1 {1 1 1}              // where {1 1 1} is the first  E1
    list line
     set switch-type = switch-cas  // specify the type of signalling, in our case
     write                         // it is switch-cas for DIAL and net5-pri for ISDN
```

Smurf Amplification: The smurf Attack is a denial of service which affects both an intermediary network and a target network by causing extreme traffic congestion. The attacker begins spoofing the source addres to seem's the target address, and then it sends many echo requests to many intermediary networks broadcast addresses, slowing the intermediary networks and in the target network which will be saturated with so many echo replies sent by the used hosts in the intermediary networks.

Many echo replies are
received by the target

Target

Broadcast echo request

Intermediary Network

Source address is spoofed
to be target's address
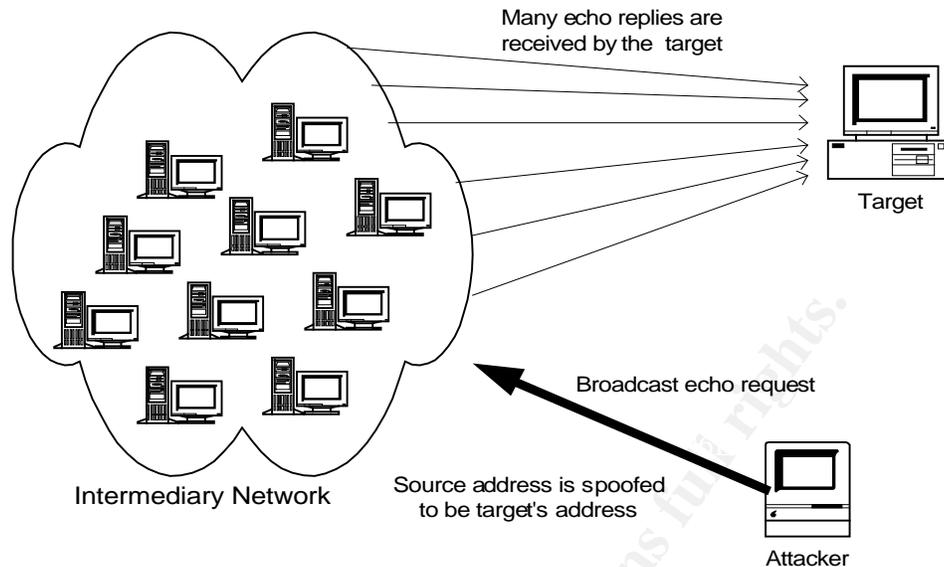
Attacker

To avoid that the MAX TNT Server is used to amplify Smurf attacks, the following commands should be applied in each interface :

read ip-int {{1 c 1} 0}   *// specify a interface*
 set directed-broadcast-allowed = no   *// disable the smurf amplification*
 write
read ip-global
 set icmp-reply-directed-bcast = no   *// disable the echo reply in the*
write   *// broadcast addresses*

Console Protection: In the default configuration the MAX TNT does not have access validation from the console port, and in most cases it is a problem, because in most places there is no local security and physical access control. Fortunately, we can insert a validation control with user and password in the console port to configure this, the following commands should be applied :

read serial { 1 17 2 }   *// specify the console port*
 set user-profile = user-def   *// specify a non-valid user, forcing*
 set auto-logout = yes   *// a prompt login*
 write

Not only the validation at the console port is sufficient in cases where there is a modem, or other similar device, attached in the console port. In these cases it is interesting to provide validation at the thelco network, we can determine the numbers allowed to call to the number attached to the modem, in this way we can enforce that only authorized people can connect to the equipment through a modem.

Source-Route Abuse: Source routing is rarely used nowadays, however it consists of allowing a sending host to exactly specify the route that a packet must take when traveling from source to destination. This specification is accomplished by including a list of the routers that must handle the datagram as it is routed through the Internet. If source route is available it is easily exploited for nefarious purposes, like in the diagram below where the target host uses the route provided in a TCP active open request for return traffic, then if the originator of the packet is hostile, the source route provides means by which packets destined for arbitrary IP addresses may be routed back to the attacker.


```
Trusted Host

The Target Host uses the
reverse of the source route
provided by the attacker in a
TCP active open request.

Attacker

intending to be
a Trusted Host

Target Host
```
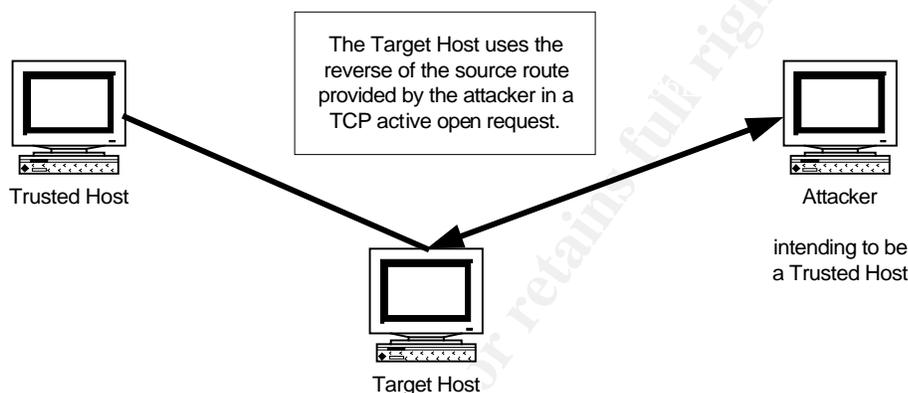
The following commands should be applied :

read ip-global
 set drop-source-routed-ip-packets = yes   *// drop source routed packets*
 set ignore-icmp-redirects = yes   *// ignore the ICMP redirects*
 set send-icmp-dest-unreachable = no   *// disable the send of the*
write   *// ICMP unreachable packets*

The first one will drop the source-routed packets, the second will avoid to use the equipment in Man-in-the-Midle Attacks, and the last is disabled to difficult the reconnaissance process.

SynFlood Attacks: Recall that in TCP three-way handshake the server responds to a client's initial SYN packet by sending a SYN-ACK. The server waits for another ACK from the client before the connection becomes established. The attack consists of a client with a spoofed address starting many TCP connections, because the server responds with the SYN-ACK and starts waiting for the ACK from the clients which is never received. As everything has a finite size, the legitimate clients will be unable to connect to the server.
To avoid synflood attacks destinated to the equipment, causing a Denial of Service, a protection to this should be activated :

read ip-global
 set tcp-syn-flood-protect = yes
 write

Terminal Server: One of the weakest security points in a RAS server, which can be vulnerable, is the access to the equipment through an E1 connection directly based on a Terminal Client. To avoid this we can configure the Terminal Server to perform an authentication and remove many of the existing Terminal features :

```
read terminal-server
 set enable = yes          // enable the terminal server, used by many ISP's
 set security-mode = full  // specify the control access level
 list terminal-mode
  set system-password = <password>  // specify a password to the terminal
  set banner = "<Banner-Message>"
  set prompt = "$"         // change the default prompt Ascend#
  set ping = no            // disable the PING from the terminal
  set traceroute = no      // disable the TRACE from the terminal
  list telnet
   set telnet = no         // disable the telnet from the terminal
  list ..
 list ..
 list menu-mode
  set start-with-menus = no    // disable the menu interaction
 list ..
 write
```

If the Terminal Server isn't necessary, it is better to disable it.

Management: It is as important as the Security is. The management system for the MAX TNT RAS Server is the software Navis Access which can run under a NT or Solaris System, unfortunatelly this management system uses only SNMP version1.

The SNMPv1 does not have any mechanism of cryptograph, then it is recommeded an out-bound and secure network destinated only to management and it is still recommended to choose SNMP string communities wich are more difficult to be broken, to change periodically the strings and to use the validation of the SNMP managers based in their IP addresses defining the rights of reading, writing or both. The Security Policy must define these tasks.

To prepare the equipment to be fully managed by Navis Access System, the following commands should be applied :

```
read snmp
 set enable = yes                          // enable the SNMP
 set read-community = <Community>          // specify the community string
 set enforce-address-security = yes        // enable the IP validation
 list read-access-hosts
  set 1 = <IP-Address-Allowed-1>           // specify the managers allowed
  set 2 = <IP-Address-Allowed-2>           // to read through SNMP
  ...
```

```
     set 8 = <IP-Address-Allowed-8>
     write
list write-access-hosts
     set 1 = <IP-Address-Allowed-1>            // specify the managers allowed
     set 2 = <IP-Address-Allowed-2>            // to write through SNMP
     ...
     set 8 = <IP-Address-Allowed-8>
     write

     new trap <Trap-Name>
     set community-name = <Community>// specify the community used for traps
     set host-address = <IP-Address-Management-Server>
     set port-enable = yes             // enable the port traps
     set slot-enable = yes             // enable the slot traps
     set security-enable = yes         // enable the security traps
     write
```

Filters : When a filter is applied to an interface, the MAX TNT monitors the data stream on that interface and takes a specified action when packet contents match the filter. Each filter can be defined in two directions : inbound and outbound, and it can have 12 rules in each direction. The order of the rules is very important, because the packet is inspected rule-to-rule in the order. If the comparison fail, the next rule will be inspected, if the comparison suceeds, the filter process stops and the defined action is taken.

There are 5 types of filters available in the MAX TNT :

1. <u>Generic Filters</u> - Can match any packet regardless of its protocol type or header fields.
2. <u>IP Filters</u> - Can work with information, like protocols of the IP family, ports, sources and destinations
3. <u>Type of Service Filters</u> - Can enable a proxy-QoS (Quality of Service) for all packets that match a especific filter
4. <u>IPX Filters</u> - Can identify specific networks, hosts or services in a Netware Network
5. <u>Route Filters</u> - Can affect only RIP packets

The first three types of filters can be implemented in a RADIUS profile too, the two others can´t. Two of them are more useful in today's networks : IP and Generic filters, because with them we can protect our networks, making blocks based of the IP header like addresses, ports, protocols and others; or based on a hexadecimal value regardless of the fields.

Generic Filters

The filter specifications operate together to define a location in a packet and an hexadecimal value to compare with it. In this way it is very useful to deny attacks with a well-known signature in their packets.

The parameters of a generic filter are :

- ◆ Type - The type of a filter, in this case it must be gen-filter
- ◆ Offset - Byte-offset at which to start comparing packet contents to the value specified in the filter
- ◆ Len - Number of bytes to test in a packet, starting at the specified off-set
- ◆ Comp-neq - Type of comparison to perform. If Comp-Neq (Compare-Not-Equals) is set to yes, the comparison succeeds if the contents do not equal the specified value.
- ◆ Mask - A binary mask. The system applies the mask to the specified value before comparing it to the bytes in a packet specified by an Offset.
- ◆ Value - An hexadecimal number to be compared to specific bits contained in packets after the Offset, Lenght and Mask calculations have been applied.

Below follows an example of a Generic filter that can deny the first Back Oriffice version attack which is based in a well-known signature, inspecting the packet. In this case the filter searches for the default secret used : "magic" which is "ce:63:d1:d2:16:e7:13:cf" in Hexa.

new filter anti-trojans

set input 1 valid = yes
set input 1 forward = no
set input 1 type = gen-filter
set input 1 ip-filter comp-neq = no
set input 1 ip-filter offset = 8
set input 1 ip-filter len = 8
set input 1 ip-filter mask = ff:ff:ff:ff:ff:ff:ff:ff
set input 1 ip-filter value = ce:63:d1:d2:16:e7:13:cf

set input 2 valid = yes
set input 2 forward = yes
set input 2 type = gen-filter

IP Filters

IP filters affect only IP and related packets, like TCP, UDP, ICMP and others. They make use of the information in the header of the packet.

The parameters of an IP filter are:

- ♦ <u>Type</u> - The type of a filter, in this case it must be ip-filter
- ♦ <u>Protocol</u> - It represents a protocol as a number, the number 0 represents any protocol. For a list of protocols see RFC 1700 "Assigned numbers", by Reynolds J. and Postel J., October 1994.
- ♦ <u>Source-Address-Mask</u> - A mask to be applied to the Source-Address before comparing.
- ♦ <u>Source-Address</u> - An IP address, which represents the source of the packet.
- ♦ <u>Dest-Address-Mask</u> - A mask to be applied to the Dest-Address before comparing.
- ♦ <u>Dest-Address</u> - An IP address, which represents the destination of the packet.
- ♦ <u>Src-Port-Cmp</u> - Type of comparison to perform when comparing source port numbers. If set to None, no comparison is made. Other values are : Less,Eql,Gtr and Neq.
- ♦ <u>Source-Port</u> - A port number to be compared with the source port of a packet.
- ♦ <u>Dst-Port-cmp</u> - Type of comparison to perform when comparing destination port numbers. If set to None, no comparison is made. Other values are : Less,Eql,Gtr and Neq.
- ♦ <u>Dest-Port</u> - A port number to be compared with the destination port of a packet.
- ♦ <u>TCP-Estab</u> - Enables/Disables application of the filter only to packets in an established TCP session.

As already said, the inspection is made rule-to-rule, and the following procedure is performed to inspect each rule :
- ♦ Apply the source-Address-Mask to the Source-Address value and compare the result to the source address in the packet. If they are not equal, the comparison fails.
- ♦ Apply the Dest-Address-Mask to the Dest-Address value and compare the result to the destination address in the packet. If they are not equal, the comparison fails.
- ♦ If the Protocol parameter is zero (wich matches any protocol), the comparison succeeds. If it is non-zero and not equal to the protocol field in the packet, the comparison fails.
- ♦ If the Src-Port-Cmp parameter is not set to None, compare the Source-Port number to the source port number of the packet. If they do not match as specified in the Srv-Port-Cmp parameter, the comparison fails.
- ♦ If the Dst-Port-Cmp parameter is not set to None, compare the Dest-Port number to the destination port number of the packet. If they do not match as specified in the Dst-Port-Cmp parameter, the comparison fails.
- ♦ If TCP-Estab is Yes and the protocol number is 6, the comparison succeeds.

Below follows an example of an IP filter that can deny some TCP and UDP ports in both directions, normally used by trojans and it can deny packets going out from the internal network with spoofed addresses too.

new filter anti-trojans-outspoof

set input 1 valid = yes	*// specify a valid INPUT rule*
set input 1 forward = no	*// define a deny action*
set input 1 type = ip-filter	*// define an IP filter*
set input 1 ip-filter protocol = 6	*// specify the TCP protocol*
set input 1 ip-filter dst-port-cmp = eql	
set input 1 ip-filter dest-port = 12345	*// specify the NetBUS default port*

set input 2 valid = yes	
set input 2 forward = no	
set input 2 type = ip-filter	
set input 2 ip-filter protocol = 17	*// specify the UDP protocol*
set input 2 ip-filter dst-port-cmp = eql	
set input 2 ip-filter dest-port = 12345	

set input 3 valid = yes	
set input 3 forward = no	
set input 3 type = ip-filter	
set input 3 ip-filter protocol = 6	
set input 3 ip-filter dst-port-cmp = eql	
set input 3 ip-filter dest-port = 31337	*// specify the BO default port*

set input 4 valid = yes	
set input 4 forward = no	
set input 4 type = ip-filter	
set input 4 ip-filter protocol = 17	
set input 4 ip-filter dst-port-cmp = eql	
set input 4 ip-filter dest-port = 31337	

set output 1 valid = yes	*// specify a valid INPUT rule*
set output 1 forward = no	
set output 1 type = ip-filter	
set output 1 ip-filter protocol = 6	
set output 1 ip-filter dst-port-cmp = eql	
set output 1 ip-filter dest-port = 12345	

set output 2 valid = yes	
set output 2 forward = no	
set output 2 type = ip-filter	
set output 2 ip-filter protocol = 17	
set output 2 ip-filter dst-port-cmp = eql	
set output 2 ip-filter dest-port = 12345	

set output 3 valid = yes
set output 3 forward = no

set output 3 type = ip-filter
set output 3 ip-filter protocol = 6
set output 3 ip-filter dst-port-cmp = eql
set output 3 ip-filter dest-port = 31337

set output 4 valid = yes
set output 4 forward = no
set output 4 type = ip-filter
set output 4 ip-filter protocol = 17
set output 4 ip-filter dst-port-cmp = eql
set output 4 ip-filter dest-port = 31337

set output 5 valid = yes
set output 5 forward = yes   *// define a permit action*
set output 5 type = ip-filter
set output 5 ip-filter dest-address-mask = 0.0.0.0
set output 5 ip-filter dest-address = 0.0.0.0
set output 5 ip-filter source-address-mask = 255.255.255.0
set output 5 ip-filter source-address = 192.168.1.0

set output 6 valid = yes
set output 6 forward = no
set output 6 type = ip-filter

Applying a filter to an interface

When you apply a filter to a WAN interface, it takes effect only when the connection is brought up, instead of a LAN interface in which the filter takes effect exactly when it is applied.

♦ To apply a filter in a WAN interface :

read connection <Connection-Name>
 set session data-filter = <Filter-Name>

*This step must be repeated for every connection in the equipment.

♦ To apply a filter in a LAN interface :

read ether {1 12 1}   *// specify the first LAN interface*
 set filter-name = < Filter-Name >

Anti-Spoofing Control: To avoid that the provided access for the MAX TNT are malicious used with spoofed address with the purpose to hack other systems, the best way is to create an ACL (Access Control List) in the router in where the MAX TNT is connected. Then any packet sourced in MAX TNT will be inspected by the router, and if it would be a spoofed packet it can be dropped.

To create the ACL the following commands should be applied in a CISCO router in the config mode.

```
config terminal
 ip access-list extended <ACL-Name>
   permit ip <Network-Address-1> <Wildcard-Network-1> any
   permit ip < Network-Address-2> <Wildcard- Network -2> any
   ....
   permit ip < Network-Address-n> <Wildcard- Network -n> any
   deny   ip any any log
```

Where : each of the sub-nets can be used as internal IP pools or as routing sub-net in the serial interfaces.

The following commands apply the ACL in an interface at the CISCO router :

```
config terminal
 interface <Interface-Id>
  ip access-group <ACL-Name> in
```

Reserved IP Ranges : A part from avoiding the spoofed outbounding packet is necessary, it's also important to avoid the inbounding IP reserved addresses packets.

Normally this kind of obstruction is made in the border routers, although, if these routers are under other's responsibility or if all the network is not protected against the outbouding spoofed packets, it is strongly recommended to create an ACL on the router in which the MAX TNT is connected to protect the equipment and its connections from reserved address wich are defined in RFC XXXX.

The following commands create an ACL for this in a CISCO router :

```
config terminal
 ip access-list extended <List-Name>
  deny   ip 0.0.0.0 0.255.255.255 any
  deny   ip 10.0.0.0 0.255.255.255 any
  deny   ip 127.0.0.0 0.255.255.255 any
  deny   ip 169.254.0.0 0.0.255.255 any
  deny   ip 172.16.0.0 0.15.255.255 any
  deny   ip 192.0.2.0 0.0.0.255 any
  deny   ip 192.168.0.0 0.0.255.255 any
  deny   ip 224.0.0.0 15.255.255.255 any
```

15

```
      deny   ip 240.0.0.0 7.255.255.255 any
      deny   ip 248.0.0.0 7.255.255.255 any
      deny   ip host 255.255.255.255 any
      permit ip any any
```

The following commands can apply the ACL in an interface of a CISCO router:

```
config terminal
 interface <Interface>
   ip access-group <List-Name> in
```

<u>Observations related to the ACL's and filters :</u>

It is important to remember that the ACL's shown before can be implemented in the MAX TNT too, without any special configuration in the router. Although it is interesting to remember two points :

1. When filters are applied in the WAN's interfaces of the MAX TNT, the connection must be restarted in order to the filter takes effect.
2. There is a limit of 12 rules in each direction in each filter in the MAX TNT.

In this way it seems better to keep some controls in the router.

Conclusion : If the MAX TNT is correctly configured, and these points are observed, the MAX TNT network is much safer, especially because the equipment has many security features, but the most of them are, in default, not set up, and many of the default enabled features are a big security threat, in this way it is very dangerous do put a MAX TNT in it's default configuration in the Internet, but there is no problem in putting it in the Internet since it has been correctly configured.

Used References :

Ascend Communications. "Ascend Max TNT – Network Configuration Guide". Part Number 7820-0547-003. Feb 2001.

Ascend Communications. "Max TNT True Access Operation System – Release Note". Oct 2000
ftp://ftp.ascend.com/pub/Software-Releases/MaxTNT/9.0.X/9.0.0/doc/maxtnt90.pdf

Cisco Systems. "Security Technologies". 17 Jun 16:34:27 PDT 1999
http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/security.htm

Cisco Systems. "Increasing Security in IP Networks". 26 Apr 15:32:59 PDT 2001
http://www.cisco.com/univercd/cc/td/doc/cisintwk/ics/cs003.htm

Jolo. "Denial of Service or "Nuke" Attacks". 21 Feb 2001
http://www.irchelp.org/irchelp/nuke/

Flavio Veloso. "The Back Orifice (BO) Protocol". 1998
http://web.cip.com.br/flaviovs/boproto.html

Carnegie Mellon University. "SMURF IP Denial-of-Service Attacks" . Jan 1998
http://www.securityfocus.com/advisories/176

Oliver Friedrichs. "TCP spoofing attack". Feb 1997
http://www.securityfocus.com/advisories/302

Recommended References :

Lucent Techonologies. "Navis Access – User Guide". Feb 2000
ftp://ftp.ascend.com/pub/Software-Releases/NavisAccess/Documentation/UserGuide_All_Platforms/NavisAccess-5-0-UserGuide.pdf

Lucent Technologies, Inc. "MaxTNT Brochure". Jan 2001
http://www.lucent.com/livelink/139863_Brochure.pdf

Upcoming SANS Training

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

SANS Paris June 2018	**Paris, FR**	**Jun 25, 2018 - Jun 30, 2018**	**Live Event**
SANS Minneapolis 2018	**Minneapolis, MNUS**	**Jun 25, 2018 - Jun 30, 2018**	**Live Event**
SANS Vancouver 2018	**Vancouver, BCCA**	**Jun 25, 2018 - Jun 30, 2018**	**Live Event**
SANS London July 2018	**London, GB**	**Jul 02, 2018 - Jul 07, 2018**	**Live Event**
SANS Cyber Defence Singapore 2018	**Singapore, SG**	**Jul 09, 2018 - Jul 14, 2018**	**Live Event**
SANS Charlotte 2018	**Charlotte, NCUS**	**Jul 09, 2018 - Jul 14, 2018**	**Live Event**
SANSFIRE 2018	**Washington, DCUS**	**Jul 14, 2018 - Jul 21, 2018**	**Live Event**
SANS Cyber Defence Bangalore 2018	**Bangalore, IN**	**Jul 16, 2018 - Jul 28, 2018**	**Live Event**
SANS Pen Test Berlin 2018	**Berlin, DE**	**Jul 23, 2018 - Jul 28, 2018**	**Live Event**
SANS Riyadh July 2018	**Riyadh, SA**	**Jul 28, 2018 - Aug 02, 2018**	**Live Event**
Security Operations Summit & Training 2018	**New Orleans, LAUS**	**Jul 30, 2018 - Aug 06, 2018**	**Live Event**
SANS Pittsburgh 2018	**Pittsburgh, PAUS**	**Jul 30, 2018 - Aug 04, 2018**	**Live Event**
SANS San Antonio 2018	**San Antonio, TXUS**	**Aug 06, 2018 - Aug 11, 2018**	**Live Event**
SANS August Sydney 2018	**Sydney, AU**	**Aug 06, 2018 - Aug 25, 2018**	**Live Event**
SANS Boston Summer 2018	**Boston, MAUS**	**Aug 06, 2018 - Aug 11, 2018**	**Live Event**
Security Awareness Summit & Training 2018	**Charleston, SCUS**	**Aug 06, 2018 - Aug 15, 2018**	**Live Event**
SANS Hyderabad 2018	**Hyderabad, IN**	**Aug 06, 2018 - Aug 11, 2018**	**Live Event**
SANS New York City Summer 2018	**New York City, NYUS**	**Aug 13, 2018 - Aug 18, 2018**	**Live Event**
SANS Northern Virginia- Alexandria 2018	**Alexandria, VAUS**	**Aug 13, 2018 - Aug 18, 2018**	**Live Event**
SANS Krakow 2018	**Krakow, PL**	**Aug 20, 2018 - Aug 25, 2018**	**Live Event**
SANS Chicago 2018	**Chicago, ILUS**	**Aug 20, 2018 - Aug 25, 2018**	**Live Event**
Data Breach Summit & Training 2018	**New York City, NYUS**	**Aug 20, 2018 - Aug 27, 2018**	**Live Event**
SANS Prague 2018	**Prague, CZ**	**Aug 20, 2018 - Aug 25, 2018**	**Live Event**
SANS Virginia Beach 2018	**Virginia Beach, VAUS**	**Aug 20, 2018 - Aug 31, 2018**	**Live Event**
SANS San Francisco Summer 2018	**San Francisco, CAUS**	**Aug 26, 2018 - Aug 31, 2018**	**Live Event**
SANS Copenhagen August 2018	**Copenhagen, DK**	**Aug 27, 2018 - Sep 01, 2018**	**Live Event**
SANS SEC504 @ Bangalore 2018	**Bangalore, IN**	**Aug 27, 2018 - Sep 01, 2018**	**Live Event**
SANS Wellington 2018	**Wellington, NZ**	**Sep 03, 2018 - Sep 08, 2018**	**Live Event**
SANS Amsterdam September 2018	**Amsterdam, NL**	**Sep 03, 2018 - Sep 08, 2018**	**Live Event**
SANS Tokyo Autumn 2018	**Tokyo, JP**	**Sep 03, 2018 - Sep 15, 2018**	**Live Event**
SANS Tampa-Clearwater 2018	**Tampa, FLUS**	**Sep 04, 2018 - Sep 09, 2018**	**Live Event**
SANS MGT516 Beta One 2018	**Arlington, VAUS**	**Sep 04, 2018 - Sep 08, 2018**	**Live Event**
SANS Cyber Defence Canberra 2018	**OnlineAU**	**Jun 25, 2018 - Jul 07, 2018**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**