SECURING YOUR NETWORK PERIMETER BY FILTERING INBOUND TRAFFIC ON ACK AND RESET BITS ON NORTEL ROUTERS.

Oleg Kirillov
February 28, 2001

OBJECTIVE:

Enhance network security by creating router filters to allow outbound TCP connection.

CIRCUMSTANCES:

There are many perimeter routers acting as firewall routers with packet filters on external interfaces facing third party companies. We can filter IP inbound traffic based on specify bit patterns in one of the following IP headers in an IP datagram:

1. The IP header
2. The header of upper-level protocol (TCP or UDP for example)

We can enhance security by creating the traffic filters with TCP ESTABLISHED criteria. This criterion is predefined for IP traffic filters.

FIX / IMPOVEMENT:

Add TCP ESTABLISHED criteria to filter that allow filtering on ACK and RESET bits in the TCP header.

BACKGROUND:

TCP is connection-oriented protocol that supports error-correction and other robust capabilities, such as packet division and sequencing. TCP guarantees reliable delivery and so it retransmits each segment if an ACK is not received in a certain period of time. To achieve this reliability, every TCP connection begins with a handshaking sequence that establishes specific parameters of the connection. Also, every packet that gets sent must be responded to with an acknowledgment before another packet will get sent.

Rather than generate special-purpose ACK packets for every TCP packet, a special bit in the TCP header is used for just this purpose. For that reason, every time a response packet is generated, the ACK bit gets set, and a marker is noted to indicate what packet the ACK is for. The very first packet in a negotiation is not acknowledging anything, and so it does not have the ACK bit set. However, every subsequent TCP packet in an exchange must have the ACK bit set for the connection to be maintained.

As you can see from the following (figure 1), before transferring data, System A must establish a logical transport layer connection with the System B. To establish this connection, TCP uses a "three-way handshake" process.

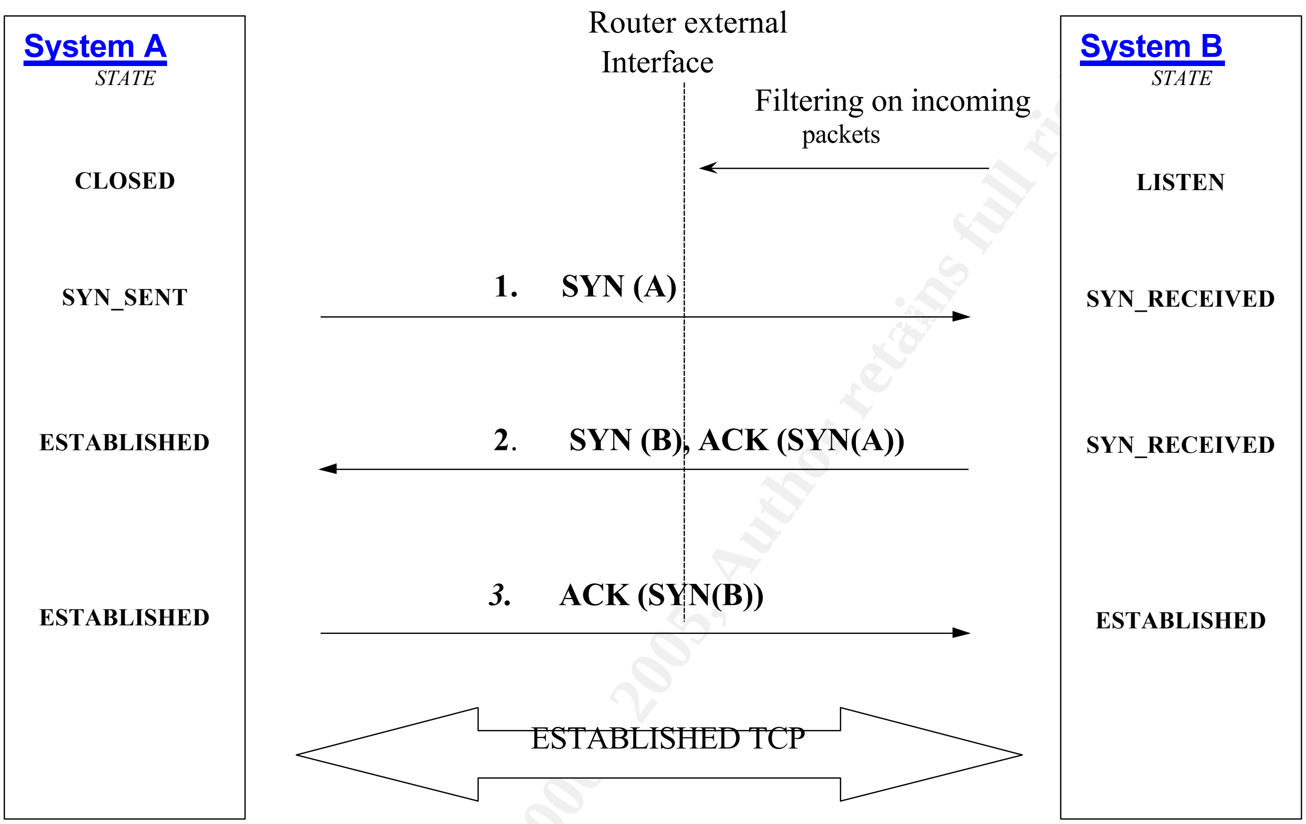


Figure 1.

1. System A sends a Protocol Data Unit (a packet) with a synchronize (SYN) bit set to 1 in its header to System B. In addition, System A assigns an Initial Sequence Number (ISN).
2. The responding TCP (System B) then sends back a PDU with both the SYN (SYN=1) bit and acknowledge (ACK=1) bit set. System B chooses its own Initial Sequence Number and puts this value in the sequence number field of the TCP segment header.
3. System A then sends to System B yet another segment (ACK=1), this last segment acknowledges System's B connection-granted segment (System A does so by putting the value System's B_ISN+1 in the acknowledgment field of the TCP segment header). The SYN bit is set to 0, since the connection is established.

During the life of a TCP connection, the TCP protocol running in each system (A and

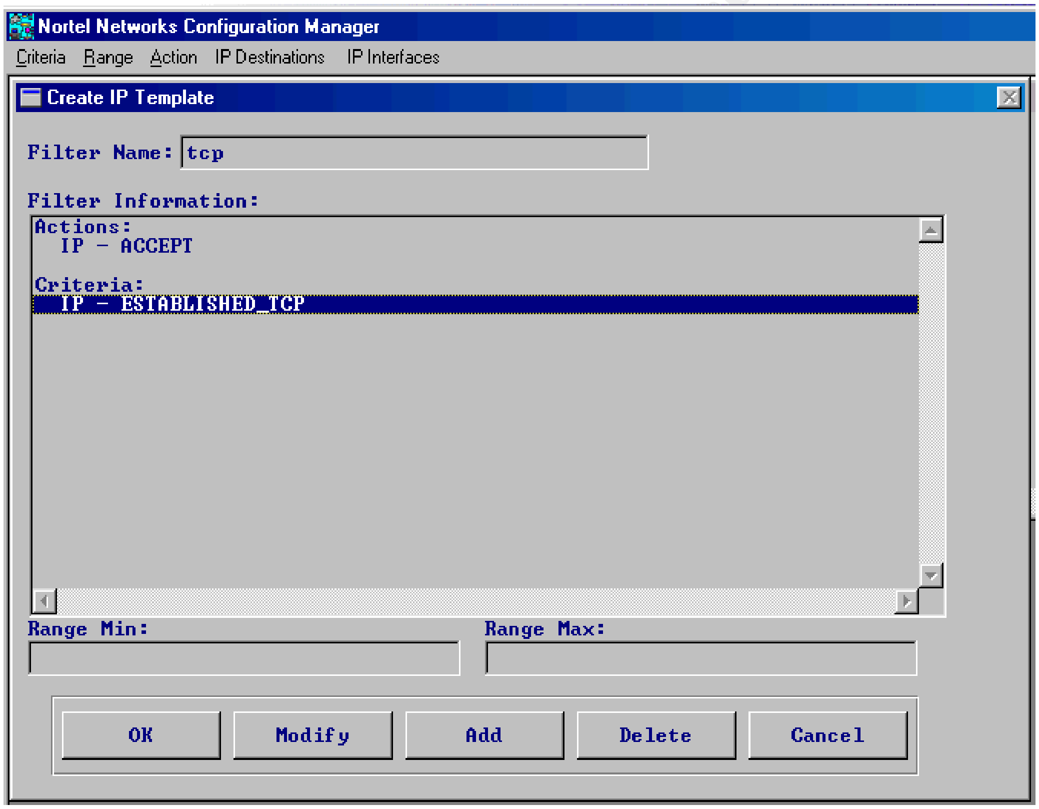
B) makes transitions through various TCP states. Figure 1 illustrates a typical sequence of TCP states from closed to listen to established.

EXAMPLES OF TCP ESTABLISHED CRITERIA

By default, the router does not filter packets on ACK and RESET bits in the IP header. To allow the router to filter on ACK and RESET bits using Bay Command Console, go to the match prompt and enter the following command:

```
match/template/template1# tcp-established on
```

TCP ESTABLISHED criteria can be specified during filter configuration with Nortel Networks Configuration Manager (figure 2.).



Filter Name: tcp

Filter Information:

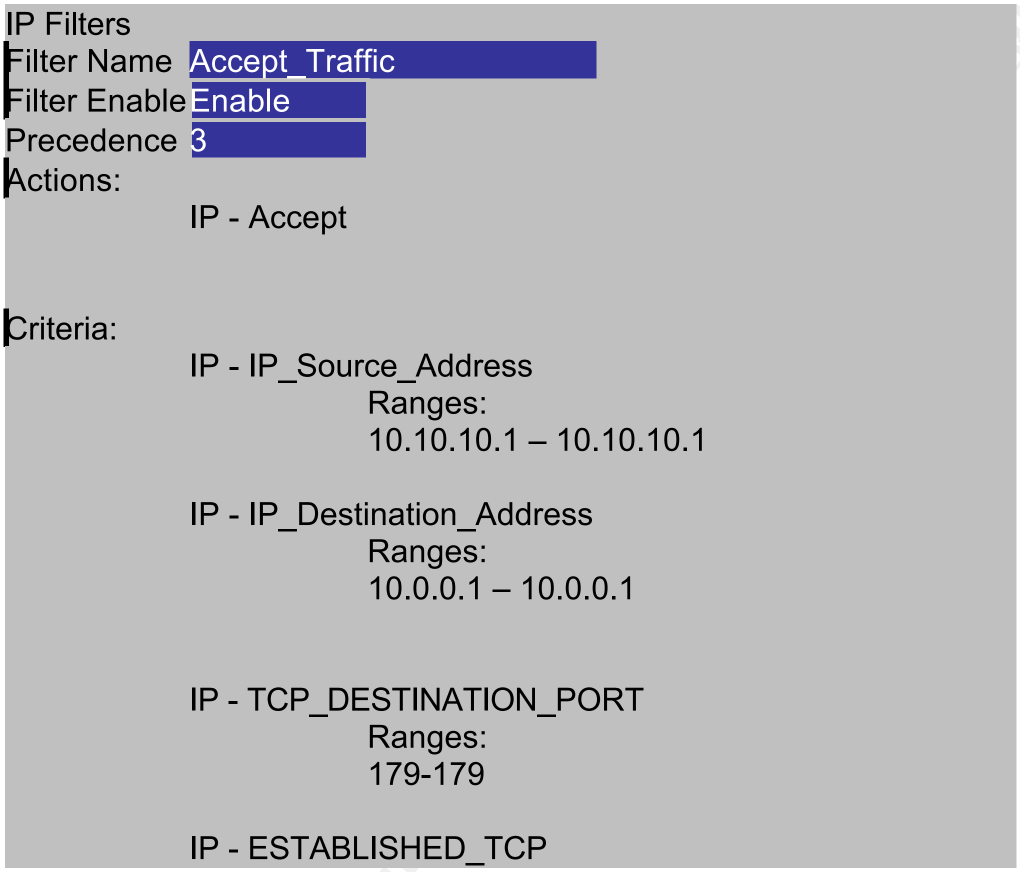
```
Actions:
  IP - ACCEPT

Criteria:
  IP - ESTABLISHED_TCP
```

Range Min:

Range Max:

Figure 2.

The following configuration sheet (Figure 3) is an example of the filter which will help you to correctly configure and implement TCP ESTABLISHED criteria for TCP-based traffic flow on the outer interface of a router.



```
IP Filters
Filter Name   Accept_Traffic
Filter Enable Enable
Precedence    3
Actions:
              IP - Accept


Criteria:
              IP - IP_Source_Address
                         Ranges:
                         10.10.10.1 – 10.10.10.1

              IP - IP_Destination_Address
                         Ranges:
                         10.0.0.1 – 10.0.0.1


              IP - TCP_DESTINATION_PORT
                         Ranges:
                         179-179

              IP - ESTABLISHED_TCP
```

Figure 3.

SUMMARY

By monitoring the ACK bit, you can limit the types of incoming data to only response packets. This means that a remote system cannot initiate a TCP connection at all, but can only respond to packets that have been sent to it. The connection can be established just from inside of the network to outside. The router will drop any attempts to established connection from outside to inside because the router will see that the packet is not an acknowledgment for a packet that it sent

REFERENCES:

1. Secure Networks Inc. “A simple TCP spoofing attack” 1997. URL
http://www.codetalker.com/advisories/sni/sni-06.html

2. Nortel Networks
http://www.nortelnetworks.com

3. Cisco Systems
http://www.cisco.com/

4. Chris Brenton. “Mastering Network Security”. SYBEX Inc., 1999.

5. Dan Blacharski. “Network Security in a Mixed Environment”. IDG Books Worldwide, Inc., 1998.