

Use switch hardware filters to enforce restrictions in a LAN and to take some of the load off of a firewall

Introduction

Network Scenario

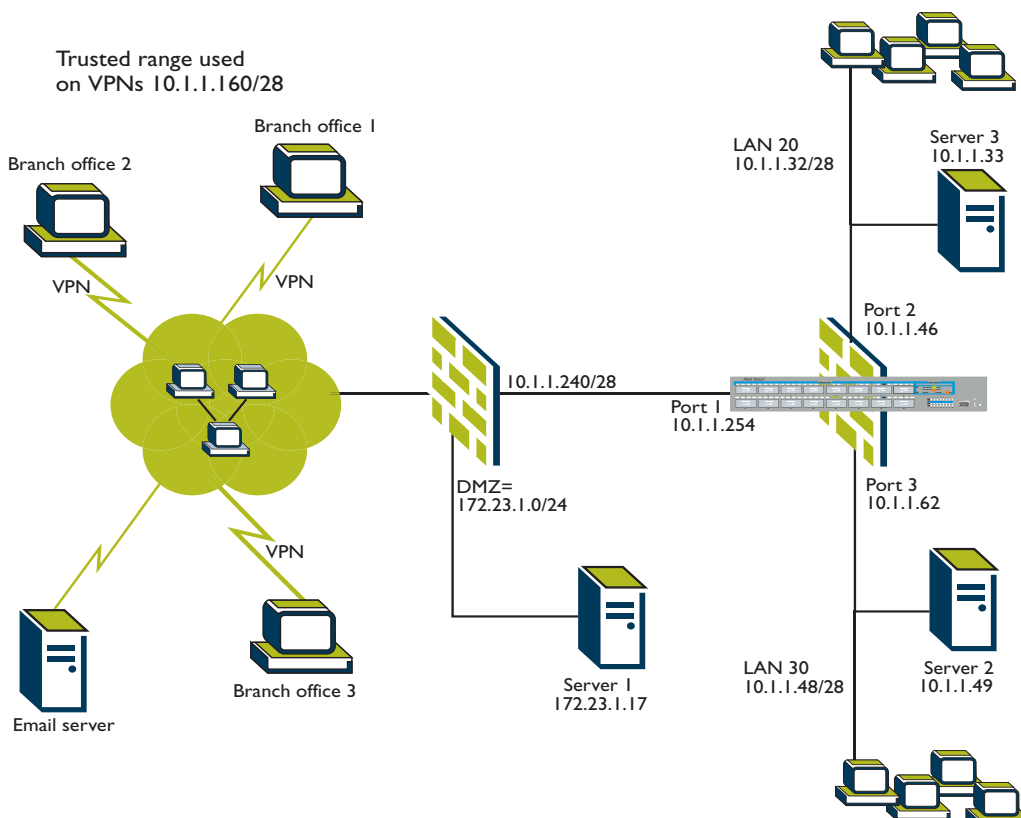
A headquarters office of a business has an Internet connection that is protected by a dedicated firewall. The LAN in behind the firewall is segmented by a Layer 3 switch, and an Allied Telesyn AT-9800 series switch.

There are two main LAN segments that terminate at the AT-9800 switch. On each of the segments there is:

- one IP subnet
- an IBM server
- some workstations

A third connection from the AT-9800 switch connects it to the firewall. Beyond the firewall, there are:

- the public Internet
- a demilitarised zone (DMZ)
- some VPN connections to other branch offices



Traffic restrictions

There are some restrictions on traffic that need to be in place on the LAN.

1. Workstations on one LAN segment can only access a limited set of applications on the server on the other segment (and vice versa).
2. Workstations and servers on the LAN segments cannot access the public Internet except to access email servers.
3. Workstations and servers on the LAN segments can access some services on the demilitarised zone (DMZ) and on the branch office networks accessed via the VPN tunnels.

Because the AT-9800 switch is the connection point between the LAN segments, it is the correct device to enforce the restrictions relating to what traffic can be exchanged between the LAN segments.

Strictly speaking, the restrictions relating to what access the LAN segments have to the DMZ, public Internet, and VPN tunnels could be enforced by the firewall. However, if the AT-9800 switch is also able to enforce those restrictions, then that will take some load off the firewall.

Additionally, there are restrictions on what externally originated traffic is allowed onto the LAN segments. The ingress of this traffic is controlled by firewall, but there is no harm in the AT-9800 switch also being configured to block undesirable ingress traffic, as a second line of defence.

The advantages of this approach

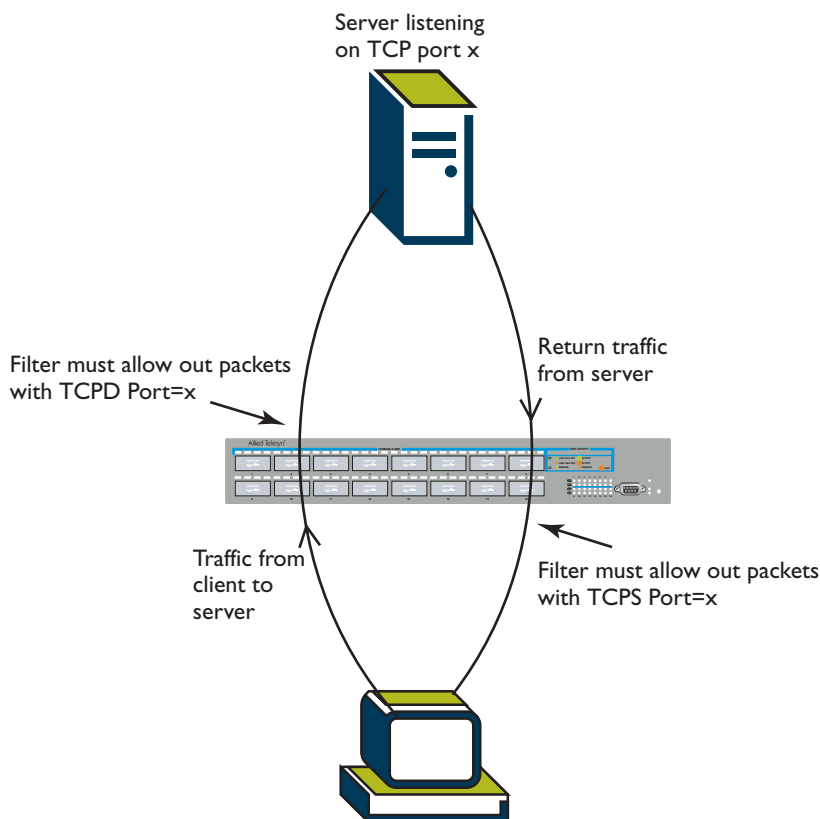
The AT-9800 switch uses hardware-based traffic filters to enforce the restrictions mentioned above. The important advantage of using hardware filtering is that it has NO impact on network performance. Even with the hardware filters in place, the AT-9800 switch will still forward traffic at gigabit rate between any pair of ports.

So, the net effect is to create a securely segmented LAN with a full gigabit of forwarding capability into and out of any given segment.

The configuration

The approach taken in creating the filtering configuration was to create rules to allow through the desired traffic between any given pair of interfaces, and then block ALL other traffic between those interfaces.

Note that if the hardware filters must allow traffic from hosts on a particular LAN to servers on another LAN, then there must be complementary filters in place to allow the return traffic from the servers back to the client hosts. So, typically, for every filter that matches on a particular destination TCP or UDP port, there will be a mirror filter that matches on that same port number as source port.



The resulting configuration script, annotated with comments, is shown below:

```
# VLAN general configuration  
#  
create vlan=dmz vid=10  
create vlan=server2 vid=20  
create vlan=server3 vid=30  
#  
# VLAN port configuration  
#  
add vlan=10 port=1  
add vlan=20 port=2  
add vlan=30 port=3
```

CLASSIFIER general configuration

```
#  
  
# Traffic from the DMZ to a COGNOS service on LAN30  
create class=10 ipsadd=172.23.1.0/24 ipdadd=10.1.1.48/28 tcpdport=9300  
  
# Traffic from the DMZ to a JBoss service on LAN30  
create class=11 ipsadd=172.23.1.0/24 ipdadd=10.1.1.48/28 tcpdport=1098  
create class=12 ipsadd=172.23.1.0/24 ipdadd=10.1.1.48/28 tcpdport=1099  
create class=13 ipsadd=172.23.1.0/24 ipdadd=10.1.1.48/28 tcpdport=4445  
  
# Traffic from the DMZ to a JSP service on LAN30  
create class=14 ipsadd=172.23.1.0/24 ipdadd=10.1.1.48/28 tcpdport=51000  
  
# Traffic from the DMZ to a Glimpse service on LAN30  
create class=15 ipsadd=172.23.1.0/24 ipdadd=10.1.1.48/28 tcpdport=2001  
  
#Traffic from remote offices to a Glimpse service on LAN30  
create class=16 ipsadd=10.1.1.160/28 ipdadd=10.1.1.48/28 tcpdport=2001  
  
#Traffic from remote offices to a Citrix service on LAN30  
create class=17 ipsadd=10.1.1.160/28 ipdadd=10.1.1.48/28 tcpdport=3389  
  
#Traffic from LAN30 to proprietary services on the firewall  
create class=19 ipsadd=10.1.1.48/28 ipdadd=10.1.1.240/28 tcpdport=4103  
create class=20 ipsadd=10.1.1.48/28 ipdadd=10.1.1.240/28 tcpdport=4105  
  
#Traffic from LAN30 to a Glimpse service on a remote office LAN  
create class=21 ipsadd=10.1.1.48/28 ipdadd=10.1.1.160/28 tcpdport=2001  
  
#Traffic from LAN30 to mail servers  
create class=22 ipsadd=10.1.1.48/28 tcpdport=25  
  
#Traffic from LAN30 to an SSH-manageable device on the DMZ  
create class=23 ipsadd=10.1.1.48/28 ipdadd=172.23.1.0/24 tcpdport=22  
  
#Traffic form LAN30 to an SQL server on LAN20  
create class=24 ipsadd=10.1.1.48/28 ipdadd=10.1.1.32/28 tcpdport=1433  
  
#Traffic from LAN30 to a Citrix service on LAN20  
create class=25 ipsadd=10.1.1.48/28 ipdadd=10.1.1.32/28 tcpdport=3389
```

```

#Traffic from LAN30 to an LDAP service on LAN20
create class=26 ipsadd=10.1.1.48/28 ipdadd=10.1.1.32/28 tcpdport=389

#Traffic from LAN30 to another proprietary service on the firewall
create class=27 ipsadd=10.1.1.48/28 ipdadd=10.1.1.240/28 tcpsport=4107
#Traffic from LAN30 to public DNS servers
create class=28 ipsadd=10.1.1.48/28 ipdadd=202.32.1.5/32 tcpdport=53
create class=29 ipsadd=10.1.1.48/28 ipdadd=202.27.4.213/32 tcpdport=53
create class=30 ipsadd=10.1.1.48/28 ipdadd=202.32.1.5/32 udpdport=53
create class=31 ipsadd=10.1.1.48/28 ipdadd=202.27.4.213/32 udpdport=53

# Return traffic from a COGNOS service on LAN30 to the DMZ
create class=110 ipsadd=10.1.1.48/28 ipdadd=172.23.1.0/24 tcpsport=9300

#Return traffic from a JBoss service on LAN30 to the DMZ
create class=111 ipsadd=10.1.1.48/28 ipdadd=172.23.1.0/24 tcpsport=1098
create class=112 ipsadd=10.1.1.48/28 ipdadd=172.23.1.0/24 tcpsport=1099
create class=113 ipsadd=10.1.1.48/28 ipdadd=172.23.1.0/24 tcpsport=4445

#Return traffic from a JSP service on LAN30 to the DMZ
create class=114 ipsadd=10.1.1.48/28 ipdadd=172.23.1.0/24 tcpsport=51000

# Return traffic from a Glimpse service on LAN30 to the DMZ
create class=115 ipsadd=10.1.1.48/28 ipdadd=172.23.1.0/24 tcpsport=2001

#Return traffic from a Glimpse service on LAN30 to the remote offices
create class=116 ipsadd=10.1.1.48/28 ipdadd=10.1.1.160/28 tcpsport=2001

#Return traffic from a Citrix service on LAN30 to the remote offices
create class=117 ipsadd=10.1.1.48/28 ipdadd=10.1.1.160/28 tcpsport=3389

#Return traffic from proprietary services on the firewall to LAN30
create class=119 ipsadd=10.1.1.240/28 ipdadd=10.1.1.48/28 tcpsport=4103
create class=120 ipsadd=10.1.1.240/28 ipdadd=10.1.1.48/28 tcpsport=4105

#Return traffic from a Glimpse service on a remote office LAN to LAN30
create class=121 ipsadd=10.1.1.160/28 ipdadd=10.1.1.48/28 tcpsport=2001

#Return traffic from an SSH-manageable device on the DMZ to LAN30
create class=123 ipsadd=172.23.1.0/24 ipdadd=10.1.1.48/28 tcpsport=22

```

```

#Return traffic from an SQL server on LAN20 to LAN30
create class=124 ipsadd=10.1.1.32/28 ipdadd=10.1.1.48/28 tcpsport=1433

#Return traffic from a Citrix service on LAN20 to LAN30
create class=125 ipsadd=10.1.1.32/28 ipdadd=10.1.1.48/28 tcpsport=3389
#Return traffic from an LDAP service on LAN20 to LAN30
create class=126 ipsadd=10.1.1.32/28 ipdadd=10.1.1.48/28 tcpsport=389

#Return traffic from another proprietary service on the firewall to LAN30
create class=127 ipsadd=10.1.1.240/28 ipdadd=10.1.1.48/28 tcpdport=4107

#Return traffic from public DNS servers to LAN30
create class=128 ipsadd=202.32.1.5/32 ipdadd=10.1.1.48/28 tcpsport=53
create class=129 ipsadd=202.27.4.213/32 ipdadd=10.1.1.48/28 tcpsport=53
create class=130 ipsadd=202.32.1.5/32 ipdadd=10.1.1.48/28 udpsport=53
create class=131 ipsadd=202.27.4.213/32 ipdadd=10.1.1.48/28 udpsport=53

#Traffic from the DMX to LAN30
create class=200 ipsadd=172.23.1.0/24 ipdadd=10.1.1.48/28

#Traffic from the Firewall to LAN30
create class=201 ipsadd=10.1.1.160/28 ipdadd=10.1.1.48/28

#Traffic from LAN30 to the DMZ
create class=202 ipsa=10.1.1.48/28 ipda=172.23.1.0/24

#Traffic from LAN30 to LAN20
create class=203 ipsadd=10.1.1.48/28 ipdadd=10.1.1.32/28

#Traffic from LAN20
create class=204 ipsadd=10.1.1.32/28

#Traffic from LAN30
create class=206 ipsadd=10.1.1.48/28
#
# SWITCH (post-VLAN) configuration
#
#Allow certain flows into LAN30
add switch hwfilter classifier=10 action=forward dport=3
add switch hwfilter classifier=11 action=forward dport=3
add switch hwfilter classifier=12 action=forward dport=3

```

```
add switch hwf classifier=13 action=forward dport=3
add switch hwfilter classifier=14 action=forward dport=3
add switch hwfilter classifier=15 action=forward dport=3
add switch hwfilter classifier=16 action=forward dport=3
add switch hwfilter classifier=17 action=forward dport=3
#Allow certain flows out to the Firewall
add switch hwfilter classifier=19 action=forward dport=1
add switch hwfilter classifier=20 action=forward dport=1
add switch hwfilter classifier=21 action=forward dport=1
add switch hwfilter classifier=22 action=forward dport=1
add switch hwfilter classifier=23 action=forward dport=1

#Allow certain flows into LAN20
add switch hwfilter classifier=24 action=forward dport=2
add switch hwfilter classifier=25 action=forward dport=2
add switch hwfilter classifier=26 action=forward dport=2

#Allow traffic to service on the Firewall
add switch hwfilter classifier=27 action=forward dport=1

#Allow DNS traffic out
add switch hwfilter classifier=28 action=forward dport=1
add switch hwfilter classifier=29 action=forward dport=1
add switch hwfilter classifier=30 action=forward dport=1
add switch hwfilter classifier=31 action=forward dport=1

#Allow return traffic out to the Firewall
add switch hwfilter classifier=110 action=forward dport=1
add switch hwfilter classifier=111 action=forward dport=1
add switch hwfilter classifier=112 action=forward dport=1
add switch hwfilter classifier=113 action=forward dport=1
add switch hwfilter classifier=114 action=forward dport=1
add switch hwfilter classifier=115 action=forward dport=1
add switch hwfilter classifier=116 action=forward dport=1
add switch hwfilter classifier=117 action=forward dport=1

#Allow return traffic into LAN30
add switch hwfilter classifier=119 action=forward dport=3
add switch hwfilter classifier=120 action=forward dport=3
add switch hwfilter classifier=121 action=forward dport=3
add switch hwfilter classifier=123 action=forward dport=3
add switch hwfilter classifier=124 action=forward dport=3
```

```
add switch hwfilter classifier=125 action=forward dport=3
add switch hwfilter classifier=126 action=forward dport=3
add switch hwfilter classifier=127 action=forward dport=3
add switch hwfilter classifier=200 action=discard dport=3
add switch hwfilter classifier=201 action=discard dport=3

#Block traffic between LANs
add switch hwfilter classifier=202 action=discard dport=1
add switch hwfilter classifier=203 action=discard dport=2
add switch hwfilter classifier=204 action=discard dport=1
add switch hwfilter classifier=205 action=discard dport=1
add switch hwfilter classifier=206 action=discard dport=1

#Allow return traffic from DNS servers into LAN30
add switch hwfilter classifier=128 action=forward dport=3
add switch hwfilter classifier=129 action=forward dport=3
add switch hwfilter classifier=130 action=forward dport=3
add switch hwfilter classifier=131 action=forward dport=3

# IP configuration
#
enable ip
add ip interface=vlan10 ip=10.1.1.254 mask=255.255.255.240
add ip interface=vlan20 ip=10.1.1.46 mask=255.255.255.240
add ip interface=vlan30 ip=10.1.1.62 mask=255.255.255.240
add ip route=0.0.0.0 mask=0.0.0.0 interface=vlan10 nexthop=10.1.1.241
add ip route=172.23.1.0 mask=255.255.255.0 interface=vlan10 nexthop=10.1.1.241
```



Only nature can do better