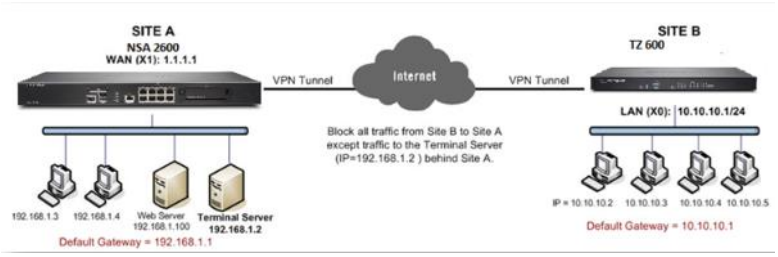
How to control / restrict traffic over a site to site VPN tunnel using Access Rules

KNOWLEDGE DATABASE

How to control / restrict traffic over a site to site VPN tunnel using Access Rules

This article illustrates how to restrict traffic to a particulare IP Address and /or a Server over a site to site VPN tunnel. This way of controlling VPN traffic can be achieved by Access Rules.



For this scenario it is assumed that a site to site VPN tunnel between an NSA 2600 and a TZ 600 has been established and the tunnel up with traffic flowing both ways.
Now, all traffic from the the hosts behind the TZ 600 should be blocked except Terminal Services (RDP traffic to a Terminal Server behind the NSA 2600.
On the other hand, the hosts behind the NSA 2600 should be able to access everything behind the TZ 600 . The configuration of each firewall is the following:

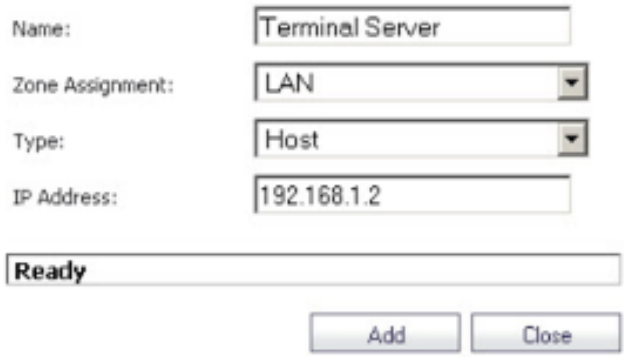
Site A (NSA 2600)
WAN (X1) IP: 1.1.1.1
LAN: 192.168.1.0/24

Site B (tz 600)
WAN (X1) IP: 2.2.2.2
LAN: 10.10.10.0/24

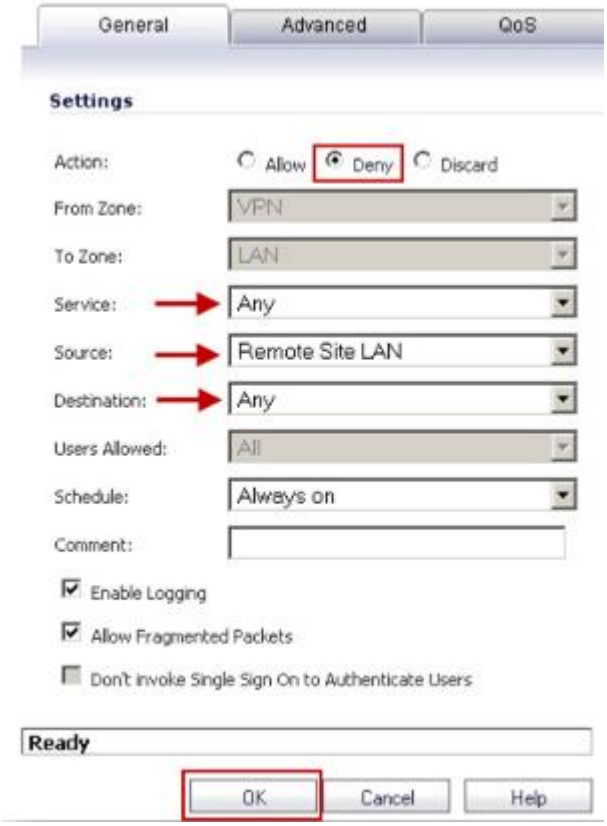
Terminal Server IP: 192.168.1.2
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.1.1 (X0 ip)

Procedure:
Step 1. Login to the Sonicwall Management Interface.

Step 2. Navigate to the **Network | Address Objects** page.
Step 3. Create a new Address Object for the Terminal Server IP Address 192.168.1.2.



Step 4. Navigate to the **Firewall | Access Rules** page.
Step 5. Select **From VPN | To LAN** from the drop-down list or matrix.
Step 6. Create a **Deny** rule blocking all traffic from the remote site with details as per the screenshot. This will override the auto-created allow rule.



Calle 146 #7-64. Bogotá D.C. Colombia
+57 1 466 0599 / +57 315 786 8258
sales@itclatam.com / tss@itclatam.com

Step 7. Create an **Allow** rule with **Source** as the address object for the Remote Site, **Destination** as the address object for the Terminal Server IP Address and **Service** as Terminal Services.

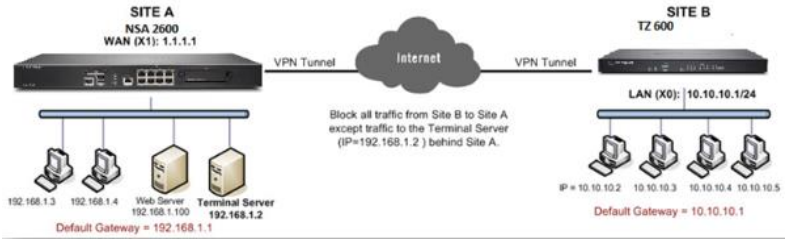
How to Test:

- From a host behind the TZ 600 , RDP to the Terminal Server IP 192.168.1.2.
- Pinging other hosts behind the NSA 2600 should fail.
- Likewise, hosts behind the NSA 2600 will be able to ping all hosts behind the TZ 600.

RESOLUTION FOR SONICOS 6.5 AND LATER

SonicOS 6.5 was released September 2017. This release includes significant user interface changes and many new features that are different from the SonicOS 6.2 and earlier firmware. The below resolution is for customers using SonicOS 6.5 and later firmware.

This article illustrates how to restrict traffic to a particulare IP Address and /or a Server over a site to site VPN tunnel. This way of controlling VPN traffic can be achieved by Access Rules.



For this scenario it is assumed that a site to site VPN tunnel between an NSA 2600 and a TZ 600 has been established and the tunnel up with traffic flowing both ways.
Now, all traffic from the the hosts behind the TZ 600 should be blocked except Terminal Services (RDP traffic to a Terminal Server behind the NSA 2600.)
On the other hand, the hosts behind the NSA 2600 should be able to access everything behind the TZ 600 . The configuration of each firewall is the following:

Site A (NSA 2600)
WAN (X1) IP: 1.1.1.1
LAN: 192.168.1.0/24

Site B (tz 600)
WAN (X1) IP: 2.2.2.2
LAN: 10.10.10.0/24

Terminal Server IP: 192.168.1.2
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.1.1 (X0 ip)

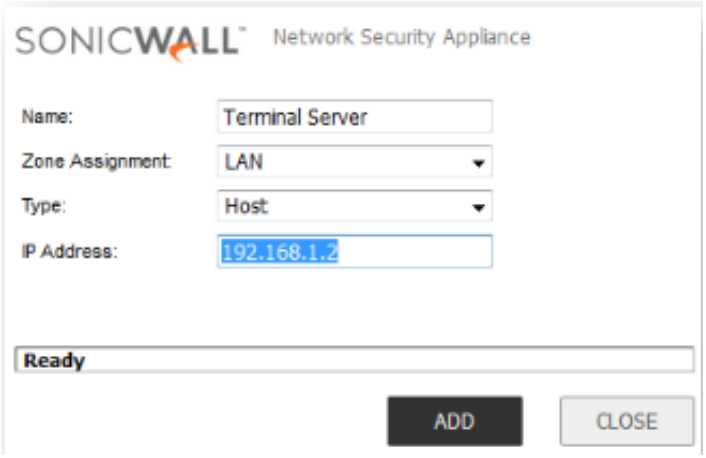
Default gateway of hosts: 10.10.10.1 (X0 ip)

Procedure:

Step 1. Login to the Sonicwall Management Interface on the NSA 2600 device.

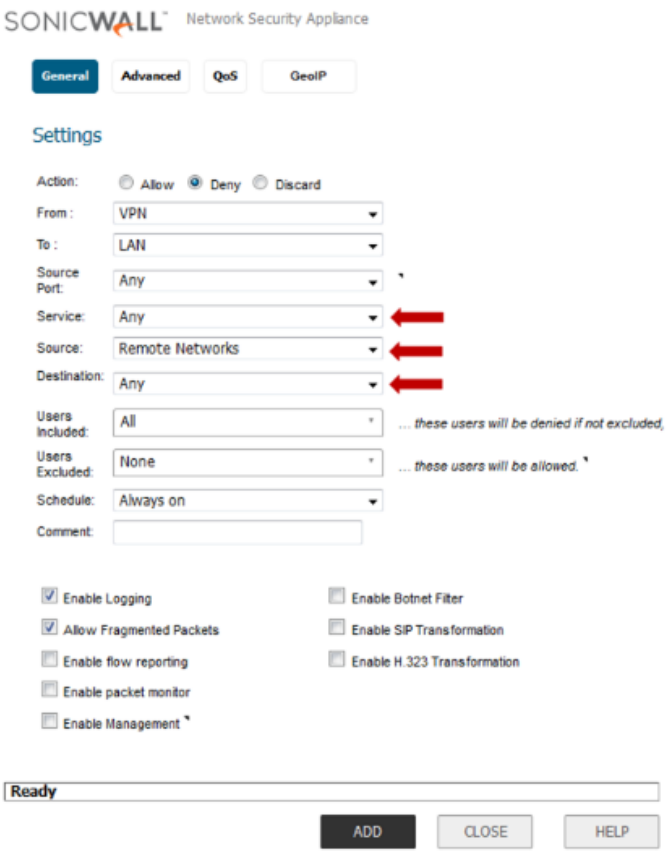
Step 2. Click **Manage** in the top navigation menu

Step 3. Navigate to the **Policies | Objects | Address Objects page.** Create a new **Address Object** for the Terminal Server IP Address 192.168.1.2.

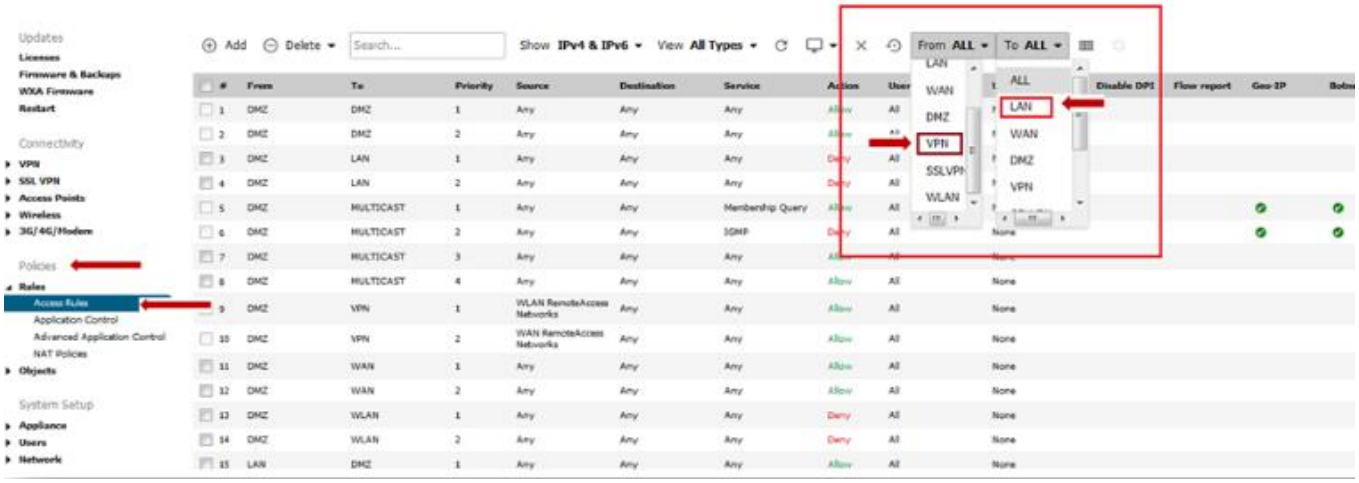


Step 4. Navigate to the **Policies | Rules | Access Rules** page.

Step 5. Select **From VPN** To **LAN** as shown in the screenshot



Step 7. Create an **Allow** rule with **Source** as the address object for the Remote Site, **Destination** as the address object for the Terminal Server IP Address and **Service** as Terminal Services.



Step 6. Create a **Deny** rule blocking all traffic from the remote site with details as per the screenshot. This will override the auto-created allow rule.

How to Test:

- From a host behind the TZ 600 , RDP to the Terminal Server IP 192.168.1.2.
- Pinging other hosts behind the NSA 2600 should fail.
- Likewise, hosts behind the NSA 2600 will be able to ping all hosts behind the TZ 600.

Calle 146 #7-64. Bogotá D.C. Colombia
+57 1 466 0599 / +57 315 786 8258
sales@itclatam.com / tss@itclatam.com