

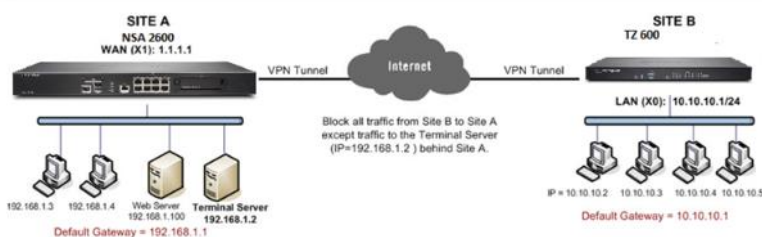


**How to control / restrict traffic
over a site to site VPN tunnel
using Access Rules**

**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 particular 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.

Name:

Zone Assignment:

Type:

IP Address:

Ready

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.

General Advanced QoS

Settings

Action: Allow Deny Discard

From Zone:

To Zone:

Service:

Source:

Destination:

Users Allowed:

Schedule:

Comment:

Enable Logging

Allow Fragmented Packets

Don't Invoke Single Sign On to Authenticate Users

Ready

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.

Settings

Action: Allow Deny Discard

From Zone: VPN

To Zone: LAN

Service: Terminal Services

Source: Remote Site LAN

Destination: Terminal Server

Users Allowed: All

Schedule: Always on

Comment:

Enable Logging

Allow Fragmented Packets

Don't invoke Single Sign On to Authenticate Users

Ready

OK Cancel Help

How to Test:

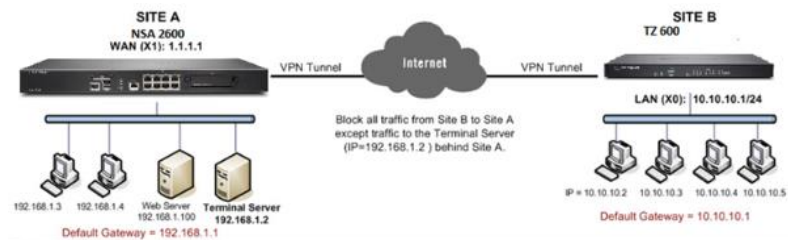
- From a host behind the TZ 600 , RDP to the Terminal Server IP 192.168.1.2.
- Pinging other hosts behind the NSA 2600 should fail.
- Likewise, hosts behind the NSA 2600 will be able to ping all hosts behind the TZ 600.

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 particular 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)

Settings

Action: Allow Deny Discard

From: VPN

To: LAN

Source Port: Any

Service: Any

Source: Remote Networks

Destination: Any

Users Included: All ... these users will be denied if not excluded.

Users Excluded: None ... these users will be allowed.

Schedule: Always on

Comment:

Enable Logging Enable Botnet Filter

Allow Fragmented Packets Enable SIP Transformation

Enable flow reporting Enable H.323 Transformation

Enable packet monitor

Enable Management

Ready

ADD CLOSE HELP

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.

SONICWALL® Network Security Appliance

Name: Terminal Server

Zone Assignment: LAN

Type: Host

IP Address: 192.168.1.2

Ready

ADD CLOSE

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.

Updates

Licenses

Firmware & Backups

WSA Firmware

Restart

Connectivity

VPN

SSL VPN

Access Points

Wireless

3G/4G/Modem

Policies

Rules

Access Rules

Application Control

Advanced Application Control

NAT Policies

Objects

System Setup

Appliance

Users

Network

#	From	To	Priority	Source	Destination	Service	Action	User	Flow report	Geo-IP	Botnet
1	DMZ	DMZ	1	Any	Any	Any	Allow	All			
2	DMZ	DMZ	2	Any	Any	Any	Allow	All			
3	DMZ	LAN	1	Any	Any	Any	Deny	All			
4	DMZ	LAN	2	Any	Any	Any	Deny	All			
5	DMZ	MULTICAST	1	Any	Any	Membership Query	Allow	All			
6	DMZ	MULTICAST	2	Any	Any	IGMP	Deny	All			
7	DMZ	MULTICAST	3	Any	Any	Any	Allow	All			
8	DMZ	MULTICAST	4	Any	Any	Any	Allow	All			
9	DMZ	VPN	1	WLAN RemoteAccess Networks	Any	Any	Allow	All			
10	DMZ	VPN	2	WAN RemoteAccess Networks	Any	Any	Allow	All			
11	DMZ	WAN	1	Any	Any	Any	Allow	All			
12	DMZ	WAN	2	Any	Any	Any	Allow	All			
13	DMZ	WLAN	1	Any	Any	Any	Deny	All			
14	DMZ	WLAN	2	Any	Any	Any	Deny	All			
15	LAN	DMZ	1	Any	Any	Any	Allow	All			

How to Test:

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.

- 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.