

# ***Citadel Firewall Configuration for VSP Service***



# Allow SMTP traffic from VSP- rule 1

## Firewall Rules ( SMTP\_IN )

Firewall Rules can accept, reject or drop packets based on the addresses, services, and/or interfaces. The order of the rules is important, since the first matching rule will determine the action for the network traffic.

Descriptive Name :

Action :

Incoming Interface :

Source IP Address/Hostname :

Outgoing Interface :

Destination IP Address/Hostname :

IP Protocol :

Service Port :

Log Enabled :

Select	Descriptive Name	Action	Incoming Interface	Source	Outgoing Interface	Destination	Protocol	Services	Log Enabled
--------	------------------	--------	--------------------	--------	--------------------	-------------	----------	----------	-------------

# Allow SMTP traffic from VSP- rule 2

## Firewall Rules ( SMTP\_IN )

Firewall Rules can accept, reject or drop packets based on the addresses, services, and/or interfaces. The order of the rules is important, since the first matching rule will determine the action for the network traffic.

Descriptive Name : Allow\_VSP\_IN2

Action : Accept

Incoming Interface : ANY

Source IP Address/Hostname : 212.79.238.64/26

Outgoing Interface : LAN

Destination IP Address/Hostname : Type your local mail server IP

IP Protocol : TCP

Service Port : SMTP

Log Enabled :

Insert

Select	Descriptive Name	Action	Incoming Interface	Source	Outgoing Interface	Destination	Protocol	Services	Log Enabled
--------	------------------	--------	--------------------	--------	--------------------	-------------	----------	----------	-------------

Delete

Move Up

Move Down

# Allow SMTP traffic from VSP- rule 3

**Firewall Rules ( SMTP\_IN )**

Firewall Rules can accept, reject or drop packets based on the addresses, services, and/or interfaces. The order of the rules is important, since the first matching rule will determine the action for the network traffic.

Descriptive Name : Allow\_VSP\_IN3

Action : Accept ▾

Incoming Interface : ANY ▾

Source IP Address/Hostname : 193.28.13.0/24

Outgoing Interface : LAN ▾

Destination IP Address/Hostname : Type your local mail server IP

IP Protocol : TCP ▾

Service Port : SMTP ▾

Log Enabled :

**Insert**

Select	Descriptive Name	Action	Incoming Interface	Source	Outgoing Interface	Destination	Protocol	Services	Log Enabled
--------	------------------	--------	--------------------	--------	--------------------	-------------	----------	----------	-------------

**Delete** **Move Up** **Move Down**

# Deny all SMTP traffic - rule 4

## Firewall Rules ( SMTP\_IN )

Firewall Rules can accept, reject or drop packets based on the addresses, services, and/or interfaces. The order of the rules is important, since the first matching rule will determine the action for the network traffic.

Descriptive Name : Deny\_SMTP\_IN

Action : Drop

Incoming Interface : ANY

Source IP Address/Hostname :

Outgoing Interface : LAN

Destination IP Address/Hostname :

IP Protocol : TCP

Service Port : SMTP

Log Enabled :

Insert

Select	Descriptive Name	Action	Incoming Interface	Source	Outgoing Interface	Destination	Protocol	Services	Log Enabled
--------	------------------	--------	--------------------	--------	--------------------	-------------	----------	----------	-------------

Delete

Move Up

Move Down

# Rules Order and Summary

## Firewall Rules ( SMTP\_IN )

Firewall Rules can accept, reject or drop packets based on the addresses, services, and/or interfaces. The order of the rules is important, since the first matching rule will determine the action for the network traffic.

Descriptive Name :

Action :

Incoming Interface :

Source IP Address/Hostname :

Outgoing Interface :

Destination IP Address/Hostname :

IP Protocol :

Service Port :

Log Enabled :

**Insert**

Select	Descriptive Name	Action	Incoming Interface	Source	Outgoing Interface	Destination	Protocol	Services	Log Enabled
<input checked="" type="radio"/>	Allow_VSP_IN1	Accept	ANY	212.79.242.192/26	LAN	-	TCP	SMTP	-
<input type="radio"/>	Allow_VSP_IN2	Accept	ANY	212.79.238.64/26	LAN	-	TCP	SMTP	-
<input type="radio"/>	Allow_VSP_IN3	Accept	ANY	193.28.13.0/24	LAN	-	TCP	SMTP	-
<input type="radio"/>	Deny_SMTP_IN	Drop	ANY	-	LAN	-	TCP	SMTP	-

**Delete**

**Move Up**

**Move Down**