

eSoft®

InstaGate Firewall Policies



Training Guide

PART ONE – UNDERSTANDING INSTAGATE FIREWALL POLICIES

1.1 Policy Overview

The eSoft InstaGate firewall offers a flexible policy editor for creating or altering the default InstaGate firewall policies. This advanced policy editor is referred to as Firewall Policy Manager and is included as a basic feature in all eSoft InstaGate products except the EX2, where it is offered as an upgrade to the basic “Passthroughs” functionality. Writing correct firewall policies is a frequently misunderstood concept, which will be explained in this document.

1.2 Default Firewall Policies

Before we begin, you should first understand the default firewall policies that the InstaGate starts with. InstaGate has a default policy of “trusting” all traffic that originates from its local networks and does not trust anything originating from untrusted networks, including the DMZ network and of course, the Internet. Firewall policies can be created to alter this default configuration.

1.3 Default NAT Policy

The InstaGate firewall will NAT (translate network addresses) all traffic that passes from its trusted networks to untrusted networks by default with all outbound traffic showing its origin as the primary firewall WAN IP as defined in the ISP WAN settings.

Multiple “secondary” IPs can be added to the outside Interface (under Network>ISP/ WAN settings>Addresses- see 1.12 below) and policies written for them, but all replies coming from the InstaGate network will respond with the primary WAN IP. This type of NAT behavior is frequently referred to as many to one NAT, multiNAT or restricted cone NAT. This NAT policy can be altered or disabled on an InstaGate firewall to accommodate other types of NAT, 1:1, many to many, or many to one NAT situations if required- see SNAT and DNAT actions below.

NAT can also be completely disabled if desired- it has a check box under the Network> ISP settings (WAN) See screen shot under 1.11 below.

1.4 Hierarchical order

Firewall policies are acted on in the order they are listed from top to bottom. As traffic passes through the firewall, packets will be inspected (headers) for matches against the policies. If no match occurs at the first rule, the second will be considered and so on. Once a policy is matched that action will be taken. SNAT and DNAT rules (see below) will be executed before accept rules.

1.5 Policy Criteria

Firewall policies can be created based on the following criteria- Source and Destination (IP and network), service port or interface. You may choose to accept, deny or use redirect (SNAT and DNAT) rules.

1.6 Network Objects

The InstaGate will predefine various network "objects" for convenience in defining commonly used networks and interfaces: WAN, LAN, WANIP, LANIP, DMZ, etc. It will add additional WANIP objects as they are added to the WAN interface- see 1.12 below. There is not a current feature to allow you to define your own.

1.7 Policy actions and priorities

Accept – Allows the service on the specified port to be accepted by the firewall or passed through to a specified IP or Network. Generally only used to allow access to firewall services or to one of its secondary IPs. It's also commonly used with a matching deny rule to define a specific outbound (LAN) policy. Another potential use would be to "lock" a particular service to one of the WAN IPs when the WAN load balancing feature is in use- this may be required for outbound SMTP mail to be accepted by a receiving server that is enforcing SPF (see SpamFilter training guide).

Redirect (DNAT) (WAN and DMZ only) – A redirect would be an allow rule followed by a redirection to an internal IP with the possibility of mapping the outgoing reply to an IP other than the WANIP if required for NAT sensitive applications. This is the most common WAN policy, allowing the firewall to pass a service through the firewall to a specified port. It is only applicable to WAN and DMZ policies.

A redirect (DNAT) policy carries a higher priority than an Accept policy, which means that a redirect policy below an allow policy for the same service will be acted on first.

Source NAT (SNAT) (WAN only) – An alternative to a general outbound accept rule that allows you to map the outbound session to a specific WAN address (other than WAN IP) for a specific destination if needed for a NAT sensitive application.

A Source NAT (SNAT) rule carries a higher priority than an accept policy from the LAN, so it will be acted on before a general accept.

Deny – Deny the service. The most common use is to create a deny policy after a specific accept policy.

Application Proxy – Application proxy is a special action for redirecting HTTP or HTTPS traffic to the web proxy. This rule is only applicable from the LAN interface. This type of rule allows you to redefine the local and remote networks that are applied when Web proxy is enabled.

1.8 System Policies

InstaGate firewall policies for system services: VPNs, email service, ping, and web proxy will appear on the Interface with an asterisk* next to the service. Some of these policies can be altered, but will potentially affect system services.

The Web proxy rule for instance enforces a browsing policy to “force” all HTTP, HTTPS traffic through the web proxy service when originating from the LAN network. This may be a policy that you choose to alter for specific workstations as in example 2 below.

Firewall: Policies						
Policies for Interface						
Interface: All						
Select	Policy Name	Action	Interface	Source	Destination	Services
<i>Click and drag to rearrange the order of the policies. When you are finished, use the Apply button to commit your changes.</i>						
<input checked="" type="radio"/>	SMTP-DMZ-WAN *	Accept	DMZ	Any	WANIP	(tcp/25)
<input type="radio"/>	SMTP-DMZ *	Accept	DMZ	Any	DMZIP	(tcp/25)
<input type="radio"/>	SMTP *	Accept	WAN	Any	WANIP	(tcp/25)
<input type="radio"/>	Web Access *	Web Access Control	LAN	Any	not LANIP	HTTP,HTTPS
<input type="radio"/>	PPTP-GRE *	Accept	WAN	Any	WANIP	(gre)
<input type="radio"/>	PPTP *	Accept	WAN	Any	WANIP	(tcp/1723)
<input type="radio"/>	IPSEC-IKE *	Accept	WAN	Any	WANIP	(udp/500)
<input type="radio"/>	IPSEC-ESP *	Accept	WAN	Any	WANIP	(esp)
<input type="radio"/>	VPNpeaktest *	Accept	LAN	192.168.1.0/24	10.10.0.0/16	All services
<input type="radio"/>	IPSEC-AH *	Accept	WAN	Any	WANIP	(ah)
<input type="radio"/>	PING-DMZ *	Accept	DMZ	Any	DMZIP	(icmp)
<input type="radio"/>	DMZ-DNS-UDP *	Accept	DMZ	Any	DMZIP	(udp/53)
<input type="radio"/>	PING *	Accept	WAN	Any	WANIP	(icmp)
<input type="radio"/>	https	Accept	WAN	Any	WANIP	HTTPS
<input type="radio"/>	VPNpeaktest-in *	Accept	WAN	10.10.0.0/16	192.168.1.0/24	All services
<input type="radio"/>	snmp	Accept	WAN	Any	WANIP	snmp
<input type="radio"/>	multipleptest	Redirect	WAN	Any	199.45.143.244/32	FTP
<input type="radio"/>	multipleptest2	Redirect	WAN	Any	199.45.143.243/32	FTP

1.9 Interface, Source, Destination

Writing a policy is easy to understand once you understand the concept. A policy will affect incoming traffic as “seen” from the designated interface. If you want to create a policy that will affect inbound traffic from the Internet, it will be a WAN policy. If you want to affect outbound traffic from the local network(s) it will be a LAN policy. Any outbound traffic from the DMZ interface will be a DMZ policy. Any inbound traffic to the DMZ network would be a WAN policy.

The source and destination will change depending on which Interface the policy is written for. A WAN policy will generally have the entire Internet (ANY) as it’s source. A LAN policy will have the local LAN network as its source. The destination will be the opposite. Choose “include” to match the defined network or “exclude” if you wish to exclude the defined network.

There are predefined network objects that can be chosen from a drop-down list which reflect the InstaGate's defined networks. You may create your own network definition using using a traditional CIDR routing syntax. Define the IP or network, and the net mask that defines the size of the network.

If you don't understand how routing works with a net mask, you might want to refer to a basic routing primer. Here's one:

<http://www.networkcomputing.com/netdesign/1122ipr.html>

Firewall: Firewall Policies

Policy Information

Name: TestPolicy

Action: Accept

Interface: WAN

Logging: Enabled

Source

Match: Include Exclude

Address or Network: Object ANY 0.0.0.0/0.0.0.0 Network

Destination

Match: Include Exclude

Address or Network: Object WANIP 192.168.1.133 / 255.255.255.255 Network

Services

All Selected

Apply Cancel

1.10 Services

Services are defined by the destination ports that they use; SMTP mail- port 25, POP3 mail- port 110, HTTP- port 80, etc. InstaGate has a list of the most common ones, but any service that can be defined by a port and transmission protocol (TCP or UDP) can be used in a policy.

Note: Typically the source port is left blank since origination ports can be changed, and are not necessary to define the service. This is done by choosing custom services under the firewall menu, and adding a service.

Services

All
 Selected

<input type="checkbox"/> America Online	<input checked="" type="checkbox"/> DNS	<input type="checkbox"/> Echo	<input type="checkbox"/> Echo Reply	<input type="checkbox"/> FTP
<input type="checkbox"/> GRE	<input type="checkbox"/> HTTP	<input type="checkbox"/> HTTPS	<input type="checkbox"/> IMAP	<input type="checkbox"/> IPSec (AH)
<input type="checkbox"/> IPSec (ESP)	<input type="checkbox"/> LDAP	<input type="checkbox"/> Lotus Notes	<input type="checkbox"/> NNTP	<input type="checkbox"/> POP
<input type="checkbox"/> Rlogin	<input type="checkbox"/> Rsh	<input type="checkbox"/> SIP	<input type="checkbox"/> SMTP	<input type="checkbox"/> SSH
<input type="checkbox"/> Secure IMAP	<input type="checkbox"/> Secure LDAP	<input type="checkbox"/> Secure News	<input type="checkbox"/> Secure POP	<input type="checkbox"/> T.120
<input type="checkbox"/> Telnet	<input type="checkbox"/> Traceroute	<input type="checkbox"/> VoIP RTC	<input type="checkbox"/> WinFrame	<input type="checkbox"/> rdp

Apply **Cancel**

Firewall: Custom Services ?

Service Name	Protocol	Source Port	Destination Port	Redirect Port
<input type="radio"/> Aim	tcp	—	5190	—
<input type="radio"/> Aim2	udp	—	5190	—
<input type="radio"/> America Online	tcp	—	5190	—
<input type="radio"/> Citrix	tcp	—	1604	—
<input type="radio"/> Citrix2	udp	—	1604	—
<input type="radio"/> Echo	icmp	—	8	—
<input type="radio"/> Echo Reply	icmp	—	—	—
<input type="radio"/> GRE	gre	—	x	—
<input type="radio"/> IMAP	tcp	—	143	—
<input type="radio"/> IPSec (AH)	ah	—	x	—
<input type="radio"/> IPSec (ESP)	esp	—	x	—
<input type="radio"/> Lotus Notes	tcp	—	1352	—
<input type="radio"/> RDP1	tcp	—	3389	—
<input type="radio"/> RDP2	udp	—	3389	—
<input type="radio"/> Rlogin	tcp	—	513	—
<input type="radio"/> Rsh	tcp	—	514	—
<input type="radio"/> Secure IMAP	tcp	—	993	—
<input type="radio"/> Secure LDAP	tcp	—	636	—
<input type="radio"/> Secure News	tcp	—	563	—
<input type="radio"/> Secure POP	tcp	—	995	—
<input type="radio"/> SSH	tcp	—	22	—
<input type="radio"/> T.120	tcp	—	1503	—
<input type="radio"/> Traceroute	icmp	—	30	—
<input type="radio"/> WinFrame	tcp	—	1494	—

Add **Modify** **Delete** **Done**

1.11 Port Address Translation (PAT)

If you have more than one internal IP that will be using the same service, you may find it useful to translate (Redirect) the destination port on the outside interface to its normal service port on the internal interface. Perhaps you have multiple desktops using a service such as RDP for instance, and you don't want to use multiple IPs to accommodate access. You can define a custom service using a port address translation which maps a chosen service port on the outside of the firewall to the regular service port (3389) on the inside so that you can accommodate multiple uses of it on the same WAN IP.

Firewall: Custom Services: Add ?

Custom Service

Name

Protocol

For most TCP/IP services the source port should be left as ANY

Source Port or Range

Destination Port or Range

Redirect Destination Port Enabled

1.12 Additional WAN IPs

You may have the need to add additional IPs to the outside Interface of the firewall to create additional policies. You may add additional IPs under the Network>WAN (ISP) settings by clicking on the addresses button. From here, you can add as many additional addresses as you own. Once added, they will appear as new objects in the firewall policies - WANIP1, WANIP2, etc.

IP Address Settings

Obtain a Dynamic IP Address

Assign a Static IP Address

IP Address

Subnet Mask

Gateway IP Address

Network Address Translation

Use Network Address Translation (NAT) (Recommended)

DNS Resolver Settings

Primary DNS IP Address

Secondary DNS IP Address (optional)

Network: ISP Settings (WAN): Secondary IP Addresses ?

Secondary Internet IP Addresses

Address to Add

IP Address

Subnet Mask

Secondary IP Addresses

PART TWO – EXAMPLES

2.1 Web Server Redirect

Suppose we had a web server on our Internal network that we'd like to make accessible from the Internet.

- This is a WAN rule, because it pertains to the WAN Interface, from which the traffic will be originating
- The action will be redirect (DNAT) to allow us to pass the traffic from the WAN to the internal IP
- You may check "logging" if you would like the firewall to log every event that matches this rule. This is only recommended for troubleshooting a problem.
- The source will be anywhere on the Internet, so we'll pick the "ANY" object which defines the source as all IPs/Networks: 0.0.0.0/ 0.0.0.0
- The destination IP will be the outside WANIP (199.45.143.116) , which is then redirected to an internal server on the local network: 192.168.100.15. The net mask assumed a single host: 255.255.255.255.
- The service is HTTP and HTTPS, which we can choose from the list of common services

The screenshot shows the configuration for a Firewall Policy named 'Webserver'. The configuration is as follows:

- Policy Information:**
 - Name: Webserver
 - Action: Redirect (DNAT)
 - Interface: WAN
 - Logging: Enabled
- Source:**
 - Match: Include
 - Address or Network: ANY (0.0.0.0 / 0.0.0.0)
- Public Destination:**
 - Traffic to this address will be redirected to the Private Destination Address.
 - Address: WANIP (199.45.143.116)
- Private Destination:**
 - Traffic originally addressed to the Public Destination Address will be sent here.
 - Address: IP Address (192.168.100.15)
- Redirect Source Address:**
 - Response traffic from the Private Destination Address normally has its source address replaced with the WAN IP Address. If the Public Destination Address is a secondary WAN IP address you may want to use that source address instead.
 - Use the default NAT rule on the WAN IP for outgoing traffic.
 - Map outgoing traffic from Private address 192.168.100.15 to the external destination address WANIP.
- Services:**
 - All
 - Selected
 - Selected services: HTTP, HTTPS

- Next we need to make sure that the rule does not have any HTTP or HTTPS rules above it that would take precedence:

Firewall: Firewall Policies

Policies for Interface

Interface: WAN

Select	Policy Name	Action	Source	Destination	Services
<i>Click and drag to rearrange the order of the policies. When you are finished, use the Apply button to commit your changes.</i>					
<input checked="" type="radio"/>	PPTP-GRE *	Accept	Any	WANIP	(gre)
<input type="radio"/>	PPTP *	Accept	Any	WANIP	(tcp/1723)
<input type="radio"/>	IMAP4 *	Accept	Any	WANIP	(tcp/143)
<input type="radio"/>	POP3 *	Accept	Any	WANIP	(tcp/110)
<input type="radio"/>	SMTP *	Accept	Any	WANIP	(tcp/25)
<input type="radio"/>	PING *	Accept	Any	WANIP	(icmp)
<input type="radio"/>	IPSEC-ESP *	Accept	Any	WANIP	(esp)
<input type="radio"/>	IPSEC-AH *	Accept	Any	WANIP	(ah)
<input type="radio"/>	SIP1 *	ACCEPT	Any	WANIP	SIP
<input type="radio"/>	RTP1 *	ACCEPT	Any	WANIP	VoIP RTC
<input type="radio"/>	TW450	Redirect	199.45.143.0/24	199.45.143.117	HTTPS,SSH
<input type="radio"/>	win2k3_rdp	Redirect	199.45.143.202	WANIP	RDP-Win2k3_rdp
<input type="radio"/>	Webmail *	Accept	Any	WANIP	(tcp/81)
<input type="radio"/>	Webserver	Redirect	ANY	WANIP	HTTP,HTTPS

Note: Policies will be processed in the order shown.

* System Service

Since it is a redirect rule, we only need to be concerned about the redirect rules above it. We see that there is another redirect above it, which includes HTTPS, so it will be acted on first. We can move our Web server rule above it, or we have the option of adding another IP to the WAN interface or create a special port translation (see above). Since this is for a web server, a special port probably wouldn't be practical unless it is for limited use for selected users. Let's move our rule above the TW450 access rule, which we can create a special port access for. We can move our rule by clicking and dragging it above the other redirect rule:

<input type="radio"/>	Webserver	Redirect	ANY	WANIP	HTTP,HTTPS
<input type="radio"/>	TW450	Redirect	199.45.143.0/24	199.45.143.117	HTTPS,SSH

2.2 LAN Proxy Bypass

Create a rule that will allow an internal server at 192.168.1.241 to "bypass" the web proxy for outbound HTTP access.

- This rule will be a LAN policy since the traffic will be coming from the local network
- The action will be accept, because we want to allow the traffic
- The source will be the IP of the server 192.168.1.241 with a net mask for a single IP 255.255.255.255
- The Destination will be all networks (the Internet) we'd define that with the ANY object unless something more specific is desired, which would be defined by entering a specific network
- The service is HTTP and HTTPS

Firewall: Firewall Policies

Policy Information

Name: Serverbypass

Action: Accept

Interface: LAN

Logging: Enabled

Source

Match: Include Exclude

Address or Network: Object Network 192.168.1.241 / 255.255.255.255

Destination

Match: Include Exclude

Address or Network: Object ANY 0.0.0.0/0.0.0.0 Network

Services

All Selected

America Online DNS Echo Echo Reply FTP

GRE HTTP HTTPS IMAP IPSec (AH)

IPSec (ESP) LDAP Lotus Notes NNTP POP

- Now we need to consider the position with other LAN rules, particularly the Web Access rule that enforces the Web proxy.

<input checked="" type="radio"/>	Web Access *	Web Access Control	Any	not LANIP	HTTP,HTTPS
<input type="radio"/>	Serverbypass	Accept	192.168.1.241	ANY	HTTP,HTTPS

- Since the new Server bypass rule is below the Web Access Control rule which prohibits HTTP and HTTPS traffic, we need to move it above. You can do this by clicking and dragging.

<input type="radio"/>	Serverbypass	Accept	192.168.1.241	ANY	HTTP,HTTPS
<input checked="" type="radio"/>	Web Access *	Web Access Control	Any	not LANIP	HTTP,HTTPS

- This policy should now be successful in allowing .241 to bypass the proxy.

2.3 A More Complex LAN Setup

We'd like to allow a block of 8 IPs- 192.168.2-.10, complete access to the Internet for all protocols, and lock down everyone else on the network from anything but web access.

- This policy will require multiple rules, since we need to first allow access and then deny the rest of the network.
- It will be a LAN policy, since the traffic will be originating from the LAN
- The first action will be to accept, from the specified IPs
- The source is the IPs, defined in a block would be best defined by a subnet of 14 IPs, starting at .1 and ending at .14, 192.168.1.0 with a subnet mask of 255.255.255.240, this net mask will also include .1 (the InstaGate) and .11-.14, so if there are computers with these IPs, they should be re-assigned if possible. If not possible, we would need to create multiple rules, which is less desirable.
- Destination address would be the Internet, ANY 0.0.0.0/0.0.0.0
- All services would be allowed.

Firewall: Firewall Policies

Policy Information

Name: AllowAll

Action: Accept

Interface: LAN

Logging: Enabled

Source

Match: Include Exclude

Address or Network: Object Network 192.168.1.0 / 255.255.255.240

Destination

Match: Include Exclude

Address or Network: Object ANY 0.0.0.0 / 0.0.0.0 Network

Services

All Selected

Apply Cancel

- Next, we need to place this rule above any restrictive rule, so we'd need to move it above the Web Access Control rule

<input checked="" type="radio"/>	Web Access *	Web Access Control	Any	not LANIP	HTTP,HTTPS
<input type="radio"/>	Serverbypass	Accept	192.168.1.241	ANY	HTTP,HTTPS
<input type="radio"/>	AllowAll	Accept	192.168.1.0/28	ANY	All services

- This rule will now allow all access for computers 192.168.1.1 through .14

<input type="radio"/>	AllowAll	Accept	192.168.1.0/28	ANY	All services
<input checked="" type="radio"/>	Web Access *	Web Access Control	Any	not LANIP	HTTP,HTTPS
<input type="radio"/>	Serverbypass	Accept	192.168.1.241	ANY	HTTP,HTTPS

- Now we need to create a rule to block access for anything else. The Web Access rule should suffice for controlling all HTTP, HTTPS access, so we need to create a similar rule to block everything else. A deny all rule for all services is not allowed by InstaGate for the entire local network, since it would also lock out access to the admin console, so we will create a rule that would deny all except the LAN interface.
- It would be a LAN rule again
- The action would be deny, since we want to deny services
- The source would be anywhere on the LAN network, or LAN object: 192.168.1.0/255.255.255.0
- The destination would be anywhere except for the LAN IP, this is the same destination as the Web Access Control rule, enter by choosing to exclude object LANIP.

Firewall: Firewall Policies

Policy Information

Name: DenyAll

Action: Deny

Interface: LAN

Logging: Enabled

Source

Match: Include Exclude

Address or Network: Object LAN 192.168.1.0 / 255.255.255.0 Network

Destination

Match: Include Exclude

Address or Network: Object LANIP 192.168.1.2 / 255.255.255.255 Network

Services

All Selected

Apply Cancel

- This rule will be OK after all other rules, since it is designed to deny anything that is not otherwise allowed.

<input type="radio"/>	AllowAll	Accept	192.168.1.0/28	ANY	All services
<input type="radio"/>	Serverbypass	Accept	192.168.1.241	ANY	HTTP,HTTPS
<input checked="" type="radio"/>	Web Access *	Web Access Control	Any	not LANIP	HTTP,HTTPS
<input type="radio"/>	DenyAll	Deny	LAN	not LANIP	All services

- Now all machines from .0 through .15 should have unrestricted access, all others have only web access through the Web proxy.

2.4 WAN Accessible Application Server Redirect

We'd like to create a rule to allow access to a particular server which runs an application which requires that all replies come from a specified IP instead of the default WAN IP. This requires that we use our choice to create an outbound mapping that originates from the same incoming IP instead of the WANIP by default. This is known as 1:1 NAT.

Here's how it's created- First we create a DNAT policy that allows the HTTP traffic to go to our Accounting web server on our secondary IP WANIP1, which we can choose as an object. After selecting the private destination IP, you will be given an opportunity to map outgoing traffic from private address (specified in the private destination) This will create a pair of firewall rules, the DNAT rule that you created and an additional system SNAT rule that will specify the matching IP to reply from.

Firewall: Firewall Policies

Policy Information

Name: AccountingWeb
 Action: Redirect (DNAT)
 Interface: WAN
 Logging: Enabled

Source

Match: Include
 Exclude
 Object
 Network

Address or Network: ANY 0.0.0.0/0.0.0.0

Public Destination

Traffic to this address will be redirected to the Private Destination Address.
 Address: Object WANIP1 199.45.143.117
 IP Address

Private Destination

Traffic originally addressed to the Public Destination Address will be sent here.
 Address: Object
 IP Address 192.168.1.16

Redirect Source Address

Response traffic from the Private Destination Address normally has its source address replaced with the WAN IP Address. If the Public Destination Address is a secondary WAN IP address you may want to use that source address instead.

Use the default NAT rule on the WAN IP for outgoing traffic.
 Map outgoing traffic from Private address 192.168.1.16 to the external destination address WANIP1.

Services

All
 Selected

America Online DNS Echo Echo Reply FTP
 GRE HTTP HTTPS IMAP IPsec (AH)
 IPsec (ESP) LDAP Lotus Notes NNTP POP
 RDP Rlogin Rsh SIP SMTP

<input type="radio"/>	AccountingWeb	Redirect	WAN	ANY	WANIP1	HTTP,HTTPS
<input type="radio"/>	AccountingWeb *	Source Redirect		192.168.1.16	Any	All services

2.5 Remote Desktop Redirect

We need create access to two workstations using RDP coming from the same IP address. This is not recommended as a good security practice, but will use for this example. This will require that we create unique ports on this interface mapped to different machines on the inside. Here we've created a port mapping on a special destination port of 17500, which is redirected to the standard port 3389 on the inside.

Firewall: Custom Services: Add

Custom Service

Name: RDP1
 Protocol: TCP
 Source Port or Range: ANY
 Destination Port or Range: 17500
 Redirect Destination Port: Enabled
 Redirected Port: 3389

Apply Cancel

This now becomes a custom service and can be used to create a policy.

<input type="radio"/>	RDP	tcp	—	3389	—
<input type="radio"/>	RDP1	tcp	—	17500	3389

We can then create a redirect (DNAT) rule with the new service that won't conflict with another from the same WAN IP. One policy will redirect RDP on port 17500, the other on the standard 3389.

<input type="radio"/>	RDP1	Redirect	WAN	ANY	WANIP	RDP1
<input type="radio"/>	RDP	Redirect	WAN	ANY	WANIP	RDP

PART THREE – SPECIAL NOTES AND QUALITY OF SERVICE

3.1 Special notes

There are some nuances to firewall policies that you should be aware of:

SNAT and DNAT (redirect) rules are acted on before accept rules. A redirect at the bottom of the rule list is as good as a redirect rule at the top, so long as there are no other redirects.

Web proxy rules - The Web proxy has two modes- transparent and authenticated. When the proxy is in transparent mode, it will act on all web requests as they pass through the proxy, regardless of the user. The second mode is authenticated proxy. This requires that the user change his browser settings to "redirect" browser sessions to the special proxy port, 8080, on the InstaGate's LAN IP. The user is required to provide username and password before accessing the Internet.

HTTPS requests – HTTP and HTTPS requests will pass through the proxy but since HTTPS requests are encrypted, their destination content is hidden from view with the web proxy in the transparent mode. In order to block HTTPS requests based on URL content, the proxy will need to be in authenticated mode and browser configured for the proxy on port 8080.

3.2 Quality of Service (QoS)

QoS is treated as a separate feature in the InstaGate, but is closely related since it is a firewall policy. QoS allows you to prioritize a particular service over another so that certain services would get faster delivery in a loaded network.

This can help with services that are time sensitive- voice data for instance. Any service that can be defined by a port number can be prioritized (High) or de-prioritized (Low), a normal setting would elect a first come first served priority. Within the High, Normal, and Low levels there is another prioritization called SFQ.

SFQ allows fair queuing/de-queuing from the same level and prevents one process from getting more than its fair share of the bandwidth. The de-queuing process pulls all packets from high priority first. Once the packets from that queue have been removed, the process will move to normal, and then finally low priority. On a saturated network connection, this de-queuing can lead to packet loss on a lower level.

QoS will also allow you to create a rate limit so that no service could take more than a predetermined amount of bandwidth before it is throttled. This can be applied to both inbound and outbound packets.

To create a policy you need to:

- Add a policy
- Select Source and Destination Networks
- Select Priority (High, Normal, Low)
 - Use caution when specifying High Priority
- Enter Rate Limit in Kilobits Per Second
 - Use caution when specifying unlimited kbps
- Select the type of traffic you are writing the policy for

Take caution when applying high priority and unlimited rate limit policies. If a high priority policy takes up all of the available bandwidth lower priority services will never be de-queued.

Remember that the Rate Limit value is in kilobits per second. Limit the bandwidth appropriately based on your total bandwidth available from your Internet service.

Firewall: Quality Of Service Policies: Add

Quality Of Service Policy Settings

Name:

Source Network: /

Destination Network: /

Priority:

Rate Limit: kbps

Services

<input type="checkbox"/> America Online	<input type="checkbox"/> DNS	<input type="checkbox"/> Echo	<input type="checkbox"/> Echo Reply	<input type="checkbox"/> FTP
<input type="checkbox"/> GRE	<input type="checkbox"/> HTTP	<input type="checkbox"/> HTTPS	<input type="checkbox"/> IMAP	<input type="checkbox"/> IPSec (AH)
<input type="checkbox"/> IPSec (ESP)	<input type="checkbox"/> LDAP	<input type="checkbox"/> Lotus Notes	<input type="checkbox"/> NNTP	<input type="checkbox"/> POP
<input type="checkbox"/> RDP-Win2k3	<input type="checkbox"/> Rlogin	<input type="checkbox"/> Rsh	<input type="checkbox"/> SIP	<input type="checkbox"/> SMTP
<input type="checkbox"/> SSH	<input type="checkbox"/> Secure IMAP	<input type="checkbox"/> Secure LDAP	<input type="checkbox"/> Secure News	<input type="checkbox"/> Secure POP
<input type="checkbox"/> T.120	<input type="checkbox"/> Telnet	<input type="checkbox"/> Traceroute	<input type="checkbox"/> VoIP RTC	<input type="checkbox"/> WinFrame
<input type="checkbox"/> rdp				

PART FOUR – TROUBLESHOOTING

4.1 Overview

Troubleshooting firewall policies is similar to troubleshooting other issues on the InstaGate. If a particular policy is not working, it is best to start by verifying that you have set it up properly. Refer back to this document when writing your first policies, if necessary.

After verifying the policy is set up properly, the system logs can be very helpful tools for determining if the InstaGate is handling traffic in the manner it is configured to. You can access the firewall log under “Support and Diagnostics” -> “System Logs”. At the top of the page is a drop-down menu, which will need to be changed to “Firewall” in order to display the InstaGate’s firewall logs for the past 7 days.

Do not be discouraged by the content of the log, the entries are rather straightforward once the syntax is understood. Each line of the Firewall log represents traffic that the InstaGate is either allowing or denying. By default the log records information on dropped packets that do not match a policy.

Logging can be enabled for specific policies in the Firewall Policy options. Be careful not to log all policies, as this can reduce system performance. Log only the policies that need troubleshooting.

```
2008 Mar 19 00:02:20 instagate PF Global DROP: IN=eth3 OUT=
MAC=00:01:4e:01:59:2b:00:15:2b:51:44:ee:08:00 SRC=212.47.219.89 DST=67.134.4.226 LEN=118
TOS=0x00 PREC=0x00 TTL=48 ID=30589 DF PROTO=TCP SPT=21 DPT=40995 WINDOW=8688 RES=0x00 ACK PSH
FIN URGP=0
2008 Mar 19 00:02:22 instagate PF Global DROP: IN=br0 OUT= PHYSIN=eth0
MAC=ff:ff:ff:ff:ff:ff:00:80:64:56:92:ad:08:00 SRC=10.42.11.157 DST=255.255.255.255 LEN=282
TOS=0x00 PREC=0x00 TTL=128 ID=54060 PROTO=UDP SPT=68 DPT=67 LEN=262
2008 Mar 19 00:02:22 instagate PF Global DROP: IN=br0 OUT= PHYSIN=eth0
MAC=ff:ff:ff:ff:ff:ff:00:14:5e:45:24:cd:08:00 SRC=10.42.11.10 DST=255.255.255.255 LEN=328
TOS=0x00 PREC=0x00 TTL=128 ID=2232 PROTO=UDP SPT=67 DPT=68 LEN=308
2008 Mar 19 00:02:23 instagate PF Global DROP: IN=eth3 OUT=
MAC=00:01:4e:01:59:2b:00:15:2b:51:44:ee:08:00 SRC=212.47.219.89 DST=67.134.4.226 LEN=118
TOS=0x00 PREC=0x00 TTL=48 ID=59998 DF PROTO=TCP SPT=21 DPT=40382 WINDOW=8688 RES=0x00 ACK PSH
FIN URGP=0
2008 Mar 19 00:02:23 instagate PF phishPROXY REJECT: IN=br0 OUT=eth3 PHYSIN=eth0
SRC=10.42.11.149 DST=194.67.52.35 LEN=48 TOS=0x00 PREC=0x00 TTL=127 ID=10243 DF PROTO=TCP
SPT=51004 DPT=80 WINDOW=8192 RES=0x00 SYN URGP=0
2008 Mar 19 00:02:24 instagate PF Global DROP: IN=br0 OUT= PHYSIN=eth0
MAC=ff:ff:ff:ff:ff:ff:00:80:64:56:92:ad:08:00 SRC=10.42.11.157 DST=255.255.255.255 LEN=282
TOS=0x00 PREC=0x00 TTL=128 ID=54062 PROTO=UDP SPT=68 DPT=67 LEN=262
```

Quality of Service happens on a per packet level. Remember this when troubleshooting bandwidth issues as packet size will have an impact on bandwidth usage and service levels.

4.2 Helpful Hints

1. In order for DNAT policies to work, the internal host must have its gateway pointing to the InstaGate.
2. Use a traffic sniffer like Wireshark to watch for traffic coming into and exiting the firewall interfaces or hosts when troubleshooting complex policy issues.
3. For secondary IP addresses, use system information to make sure aliases are assigned to the WAN interface correctly.
4. If you are creating policies for internally routed networks, make sure routing is correct first.
5. The ThreatMonitor has a tab for Firewall. This tab will give you a snapshot of your network traffic.
6. If there is a router or firewall in front of the InstaGate, make sure that the traffic you are dealing with is allowed to go to the InstaGate.
7. When creating a Custom Service, most will not need a source port specified, as traffic can come from many different source ports.

CONCLUSION

Firewall policies are not difficult to write once you learn the basics. They follow a very logical order and will become second nature after a little practice. If you have a particularly complex rule, you might want to contact eSoft support for assistance: 877-754-2986 or <http://support.esoft.com>