Configuring Packet Filtering and Routing Rules

CERTIFICATION OBJECTIVES

10.01 Understanding Packet Filtering and Routing
10.02 Creating and Managing Packet Filtering
10.03 Configuring Intrusion Detection
10.04 Creating and Managing Routing Rules
Q&A Self Test
Chapter 10: Configuring Packet Filtering and Routing Rules

ISA Server provides a multi-layered firewall. If you are carefully studying this book, you have certainly heard me refer to and discuss the concept of layered firewall protection. By providing network protection at various levels of TCP/IP communication, ISA Server is able to provide robust security that can meet the strictest needs of any organization.

The lowest portion of that multi-layered firewall approach is the IP packet level. When data is sent over an IP network, it is broken down into small pieces of information, or packets. Each packet contains header information that determines the sender of the packet and its destination, along with possible other routing information. ISA Server has the capability to examine IP packets and determine if the communication is allowed on the network or not. This level of IP security, along with the other layers of firewall protection offered by ISA Server, mean that you can configure network access that is very tight and very secure.

Along with packet filtering, routing rules also come into play, so it is important to discuss these two features in tandem. In this chapter, we will explore these features as well as intrusion detection, and you will learn how to configure and manage each of them.

CERTIFICATION OBJECTIVE 10.01

Understanding Packet Filtering and Routing

One of the most important things about packet filtering and routing is to understand them. Without a firm understanding of how they work and their purpose, you are quite likely to make some configuration mistakes, as well as miss a few questions on the exam. Don’t worry though, in this section, we’ll explore packet filtering and routing and how they function together.

Packet Filtering and Access Policy

Packet filtering is considered a part of access policy, or one of the items you use to determine who can access what on the Internet, and who can access information inside your private network. Access policy also includes site and content rules and protocol rules. and with a combination of these access policy elements, you can create a secure firewall scenario. When packet filters are in place, ISA Server can
inspect each packet attempting to enter the ISA Server firewall, and either allow the packet to pass through or drop it, if it is not allowed.

Packet filtering can be enabled at the enterprise or array level. When you create your enterprise policy, you can specify that packet filtering should be enforced on every array in the enterprise, as you can see in Figure 10-1.

If packet filtering is not enforced at the enterprise policy level, then it can be enabled on each array individually as desired. However, the preferred method of using packet filters is to force them at the enterprise policy level.

### Packet Filtering and Policy

Packet filtering is considered a part of access policy, but it is not the same as site and content rules and protocol rules. It is designed to function with and provide functionality for site and content and protocol rules. When packet filtering is enabled, all IP packets are automatically blocked from entering the firewall. For security reasons, no traffic is allowed to enter until you explicitly allow it. You can think of the default packet filtering setting as “deny all.” You then create exceptions, or “allow filters,” to this setting via your rules and policy. If you want to allow HTTP traffic, you create a protocol rule that permits the traffic, according to your specifications. When you create this rule, a packet filter exception is created that allows HTTP traffic to enter the firewall. This is done at the port level. The port that handles HTTP traffic can now be dynamically opened and closed to allow all HTTP traffic. With this single rule, users can access the Internet and HTTP traffic can enter the firewall, but no other types of protocols are allowed. To allow other protocols, you configure additional rules that permit access, which create additional packet filters that allow the traffic.

![Figure 10-1: Packet filtering is forced on all arrays via this enterprise policy](image-url)
Chapter 10: Configuring Packet Filtering and Routing Rules

As you can see, packet filters are created according to the policy elements that you configure. These policy elements then create a packet filter for the necessary TCP/IP ports in order to carry out the rule. These ports can be dynamically opened or closed as needed, so the policy packet filters are often referred to as “dynamic packet filters.” You can also manually create static packet filters by using the ISA Management console. Static packet filters open an IP port and keep it open. They are useful and necessary in certain situations, such as with a DMZ network, but as a general rule, the preferred method of packet filter use is through policy.

*Administrators should occasionally create static filters to invoke some filtering need that is not available via policy elements. Otherwise, policy rules should be used to configure the firewall so that dynamic packet filters will be created. This is the preferred method and a more secure use of packet filtering. You should keep this in mind for the exam.*

**Packet Filtering and Routing**

ISA Server contains a routing feature that allows the ISA Server to act like a router – information can enter the ISA server and be routed to a different section of your network. The router usage is helpful in a number of scenarios, such as with a DMZ network or if the ISA Server needs to route information to different IP subnets. The logical question that may be running through your mind is, “What does packet filtering have to do with routing?” In technical terms, perhaps nothing, but here is the issue you need to remember – you can use packet filtering and routing together for secure firewall and routing features. If you enable routing without enabling packet filtering, your ISA Server acts as a router only and allows any traffic to pass through the firewall so it can be routed. You can think of packet filtering and routing as being at opposite ends of the scale – packet filtering blocks all packets by default while routing allows all packets by default. The two are designed to function together. Without packet filtering, routing will allow all traffic from the Internet to pass through your network.

*Using routing without packet filtering turns your ISA Server computer into a router – all ports are opened and all traffic is allowed to enter. This a security breach and not a recommended use of ISA Server. Watch out for tricky exam questions about this issue.*
EXERCISE 10-1

Packet Filters and Routing

Scenario:
You are currently training a new ISA administrator who is unsure about the way in which packet filters and routing rules function with each other. How would you describe this relationship?

Solution:

1. Packet filtering blocks all IP traffic from entering the network. Dynamic packet filters can then be created via policy that allows traffic to enter on certain ports. You can also create static packet filters as needed.

2. If routing is enabled without packet filtering, the ISA Server becomes a router, allowing all IP traffic to pass through the server. This is a security breach. However, if you use packet filtering and routing together, you gain all of the security benefits of packet filtering and the management benefits of routing.

SCENARIO & SOLUTION

| How does packet filtering block packets? | IP traffic uses IP ports. Various protocols are assigned to various logical IP ports. In order to block IP traffic, ISA Server denies access by not listening to any IP ports expect those you explicitly allow in various rules. For example, if you create a rule that allows HTTP traffic, you are creating an IP packet filter that listens on port 80 and dynamically opens and closes port 80 to allow HTTP traffic to enter. All other ports are closed unless you explicitly configure protocol rules that allow the ports to open. |
| When are static filters needed? | Static filters are most often needed in special circumstances where you want to allow some application to listen to a particular IP port and accept traffic from that port. Static packet filters are also used with certain routing scenarios, such as with a DMZ network. This use is explored in more detail later in this chapter. |
Like most components of the ISA Management console, packet filtering is rather easy to configure and manage, once you understand the concepts and the application of filters and their management. In this section, we'll explore how to enable packet filtering and how to create and configure static packet filters. Keep in mind that the preferred method of packet filter application is through policies. You can use static packet filters when necessary, but if you find yourself needing to create an excessive amount of them, you should stop and examine your enterprise policy first.

Enabling Packet Filtering

Packet filtering is enabled in one of two ways. First, it can be forced at the enterprise policy level, which I discussed in the first part of this chapter. By forcing packet filtering on all arrays at the enterprise level, packet filtering is configured and enabled on each array automatically. The second option is to enable packet filtering for each individual array if there is no enterprise policy that forces it.

Some environments that are not particularly concerned with security do not force packet filtering with the enterprise policy. They simply allow individual array administrators to configure packet filtering as needed for that array. While there is nothing inherently wrong with this approach, most environments choose a unified packet filtering enforcement approach so that there is no single security breach, or at least weaker security standard, on any one array.

To access packet filtering, expand the desired array in the ISA Management console, then expand Access Policy. You will see an IP Packet Filters folder, shown in Figure 10-2.

To enable packet filtering on the array, just right-click the IP Packet Filters folder and click Properties. On the General tab, shown in Figure 10-3, there is a check box to enable packet filtering. If you currently have an enterprise policy that forces packet filtering on the array, this option will be selected and grayed out, since you will not be allowed to disable packet filtering at the array level. You also see two
Creating and Managing Packet Filters

FIGURE 10-2
IP Packet Filters folder

FIGURE 10-3
General IP Packet Filters Properties
Chapter 10: Configuring Packet Filtering and Routing Rules

You will learn more about both of these options later in this chapter.

The Packet Filters tab, shown in Figure 10-4, has three packet filtering options that you can also enable. They are:

- **Enable filtering of IP fragments** – Some malicious attacks may use fragmented IP packets. Fragmented packets are passed through the firewall and reassembled in a harmful way. Because this is a well-known attack method, you have the option to simply drop all fragmented packets before they enter the network. This setting is a good security measure, however, you cannot use it if you want to use any kind of streaming media, since audio and video streams will be interpreted as fragmented packets and dropped.

- **Enable filtering IP options** – Some IP packets have options in the header portion of the packet which enable data to have more instructions and various network functionality. The problem is that malicious attacks may be able to hide in these options and be allowed to pass through the ISA firewall. This
filtering option allows the firewall to reject all packets that have options in their headers. This setting is probably not needed for a typical network, but if you are creating a highly secure network, then you should consider enabling this option. However, a number of IP packets may be dropped, just because they have options listed in their headers.

- Log packets from ‘Allow’ filters – This option creates a log file of every packet that is passed through the firewall from the allow filters (either dynamic or static). This can be a great troubleshooting and inspection tool, but you should only log packets as needed for a specific purpose, or you may take up a lot of server disk space with unneeded log files.

**EXERCISE 10-2**

**Enabling Packet Filtering**

**Scenario:**
You’re consulting for a company which is implementing Microsoft ISA Server. On a particular array, the company wants to enable packet filtering, along with intrusion detection and IP routing. Also, the company wants to make sure that streaming media is not blocked from passing through the firewall and they want to filter out all IP packets that have IP options in their headers. How can you configure this?

**Solution:**

1. Click Start | Programs | Microsoft ISA Server.
2. In the ISA Server Management tool, expand Servers and Arrays, then expand the desired array.
3. Expand Access Policy, then right-click IP Packet Filters and click Properties.
4. On the General tab, click the Enable Packet Filtering, Intrusion Detection, and IP Routing check boxes.
5. Click the Packet Filters tab, do not select the IP Fragments check box, since the company wants to use streaming media. Do click the IP Options check box since the company wants to configure that filtering option. Click OK to save the settings.
Creating and Managing Packet Filters

The ISA Management console helps you create and manage packet filters for your network. The following sections show you how to create and manage static packet filters.

Creating Static Packet Filters

You can easily create static packet filters with the help of a wizard. It is important to keep in mind that all filters you create with this wizard are static – they cannot dynamically open and close ports as needed. The best management method is through policies and rules. However, under some circumstances, you may need to create static packet filters in order to meet your networking needs. This is especially true if you are using mail server publishing, using custom applications, or have specific Internet usage needs that cannot be met with typical rules and policies.

One issue I would like to point out before you have the opportunity to practice creating packet filters in Exercise 10-3, is the issue of array filters vs. individual server filters. The IP Packet Filter wizard will give you the option to apply the filter you are creating to all array members or to a particular array member. In other words, you can have all array members deploy the filter or just a single one. Why would you want to choose a single array member and why does ISA break the array construct in this situation? The answer is need and security. Under most circumstances, you will create a static packet filter that allows some kind of traffic into your network. Static packet filters open ports that remain open all time, or are listened to all of the time. You may want this setting applied to the entire array, but what if you need a static packet filter to support an application that needs to listen to the Internet, but you only want to run that application on one server? There would be no reason for the other array members to use the static filter since none of them run the application. The point is that ISA gives you the option to use only one server in the array or the entire array. This means you can meet your specific needs while keeping the number of static packet filters to a minimum.

Exercise 10-3 shows you how to create a static packet filter.

EXERCISE 10-3

Creating a Static Packet Filter

1. Click Start | Programs | Microsoft ISA Server.
2. In the ISA Server Management tool, expand Servers and Arrays, then expand the desired array.


4. Right-click IP Packet Filters, then click New | Filter.

5. The New IP Packet Filter wizard appears. Enter a name for the filter, then click the Next button.

6. The Servers window asks you if the filter should apply to all servers in the array or on this individual server. Make your selection, then click Next.

7. The Filter Mode window appears. Click the desired radio button to either allow or block packet transmission, then click Next.

8. The Filter Type window appears. You have the option of creating a custom filter or a predefined filter. If you choose Custom and click Next, a Filter Settings window appears, shown in Figure 10-5, where you choose the protocol, direction, and local and remote ports for that filter. Enter the settings and click Next. If you chose a predefined filter, use the drop-down menu to select the filter you want, then click Next.

9. The Local Computer window appears, as shown in Figure 10-6. In this window, you have the option to apply the filter to the default IP addresses for each external interface on the ISA Server, to a certain external IP address, or to another computer on a perimeter (DMZ) network. Make your selection and click Next.

10. The Remote Computers window appears. You can choose to apply the filter to all remote computers or a particular remote computer. Make your selection and click Next.

11. Click Finish to save the static filter.

Creating Packet Filters for DMZ Networks

You noticed in Exercise 10-3 that you had the option to apply the packet filter to the default external interfaces, a specific IP address, or a server on a perimeter, or DMZ, network. You may recall from Chapter 2 that a DMZ – or “demilitarized zone” network, also called a perimeter network – is a segmented portion of your...
Chapter 10: Configuring Packet Filtering and Routing Rules

**FIGURE 10-5**
Enter the desired values to create the custom filter.

**FIGURE 10-6**
Choose the Local Computer setting you want to apply.
network that is kept isolated for security reasons. The DMZ is most often used when you want to publish internal servers, such as mail, Web, database, etc., to the Internet. Using a DMZ, you isolate those servers from your internal network so that traffic to those servers cannot get beyond them and to private servers, yet the DMZ servers are still available to the private network clients as well as the Internet.

For the DMZ configuration to work, a few things have to be in place. The LAT does not contain the IP addresses/ranges of the DMZ, but only the private network. You need to enable packet filtering and IP routing, and then you need to create packet filters for the servers in the DMZ, depending on the services and protocols used by those published servers. Server publishing is discussed in Chapter 12. When you publish various servers in the DMZ, you must create static packet filters on the ISA Server or array that will allow the type of traffic used on those servers. Then, ISA Server can forward those packets to the published servers in the DMZ. For example, consider Figure 10-7. I have a DMZ network that contains a mail server. The ISA Server routes SMTP traffic to the mail server in the DMZ.
Chapter 10: Configuring Packet Filtering and Routing Rules

Server array allows various packets in and out of my private network as configured, but all SMTP traffic entering the firewall is routed to the mail server in the DMZ network.

The packet filters must be statically created to accept the desired traffic, then re-route it to the server in the DMZ. Use the Packet Filter wizard and configure the options as needed for the DMZ server. Exercise 10-4 gives you an example of a DMZ configuration where an SMTP server is used in the DMZ.

EXERCISE 10-4

Creating a Packet Filter for a DMZ

To create packet filter for a DMZ network (SMTP server in this example), follow these steps:

1. Click Start | Programs | Microsoft ISA Server.
2. In the ISA Server Management tool, expand Servers and Arrays, then expand the desired array.
4. Right-click IP Packet Filters, then click New | Filter.
5. The New IP Packet Filter wizard appears. Enter a name for the filter, then click the Next button.
6. The Servers window asks you if the filter should apply to all servers in the array or on this individual server. Make your selection, then click Next.
7. The Filter Mode window appears. Click the Allow packet transmission radio button, then click Next.
8. The Filter Type window appears. Click the Predefined radio button, then click the drop-down menu. Select SMTP, then click Next.
9. The Local Computer window appears, shown in Figure 10-8. Click the This computer radio button, then enter the DMZ computer’s IP address or click Browse to locate it. Click Next.
Creating and Managing Packet Filters

10. The Remote Computers window appears. You can choose to apply the filter to all remote computers or a particular remote computer. Make your selection and click Next.

11. Click Finish to save the static filter.

Managing Packet Filters

Once you have created static packet filters, you can easily manage them and change their configuration by using the ISA Management console. In the taskpad view, select the desired filter, then click the Configure Packet Filter icon, or if you are using Advanced mode, just double-click on the filter to access the Properties pages.

As you can see in Figure 10-9, the filter’s Properties pages contain all of the settings that you configured when using the wizard. You can access each of the tabs to make changes, and you can use the General tab to temporarily disable the filter if needed. All of these settings are self-explanatory.
Chapter 10: Configuring Packet Filtering and Routing Rules

FIGURE 10-9
Make configuration changes to a filter by accessing the filter’s Properties pages.

Why would you want to restrict what remote computers can send data to a particular port or filter?

When you create packet filters, you have the option of applying the filter to all or selected remote computers. This is a security issue in a situation where you are using a custom application with another computer on the Internet, or even a computer in a particular subnet. If you know that only one or a few computers will use the filter, simply restrict the filter to those computers as an additional security measure. This way, no other remote computers can access the filter.

How many DMZ based filters will I need?

That all depends on your configuration. For any servers in the DMZ zone, you will need to create static packet filters that re-route the appropriate type of data to those servers. Depending on your DMZ, you may need to create several filters.
Certification Objective 10.03

Configuring Intrusion Detection

Microsoft ISA Server includes intrusion detection software that can detect potentially malicious attacks against your network, and provides alerts so that further action can be taken. This software recognizes common hacker IP methods for invading a network or causing server/computer malfunctions. These kinds of attacks all fall under the Denial of Service (DoS) definition. DoS attacks use IP packets and related schemes to crash a computer system.

The intrusion detection software included with ISA Server is based on technology developed by Internet Security Systems, Inc., which you can visit on the Internet at http://www.iss.net. ISS produces a number of products, and you may be interested in downloading demos.

The software provides detection support for six common types of DoS attacks, which are:

- **Windows Out-of-Band (WinNuke)** – This type of attack creates a security hole in a Windows operating system. The hacker needs the IP address of the computer or server it wants to attack. Once it has the address, the attacker attaches to TCP port 139 and floods the port with garbage IP information that the computer considers “out of bounds.” This will eventually cause the networking system in the computer to crash.

- **Land Attack** – A land attack causes a communication loop by making a computer believe it is sending IP packets to itself. The hacker gets the computer's IP address, then spoofs the address by sending SYN IP packets. The receiving computer sees its own address in the packet as if it has sent the packet to itself. So, the computer is trying to both send and acknowledge its own IP address. This eventually will crash the computer.

- **Ping of Death** – The ping of Death attack uses the Internet Control Message Protocol (ICMP) echo request to flood a computer system with a large amount of ICMP echo ping data. This flood causes a kernel buffer overflow by sending packets that are large in terms of byte size. Typical packets are 64 bytes, but
the ICMP echo ping may send packets of up to 65536 bytes. These illegal sized packets cause the buffer to overflow and the system to crash.

- IP Half Scan Attack – The IP half scan attack occurs when a remote computer does not issue an ACK packet, which is an acknowledgement, during a TCP session. Instead of the ACK packet, the attacking computer replies with an RST packet to probe the port connection that is waiting on the ACK packet. This RST packet yields information that the attacker can use the open other ports.

- UDP Bomb – The UDP bomb attack uses an illegal UDP packet containing illegal data in some of the UDP fields. This kind of attack can cause the computer to crash.

- Port Scan – The port scan attack attempts to probe the full range of IP ports, looking for open ports that can be accessed. Attackers use this method to determine what ports are running what services. They use that information to target specific attacks against active services that were discovered during the port scan.

The use of intrusion detection involves two steps. First, you enable intrusion detection and the types of attacks you want to detect, then you configure alerts that are performed should an attack be detected. See Chapter 15 to learn how to configure alerts. Exercise 10-5 shows you how to enable intrusion detection and select the intrusion methods you want to detect.

**EXERCISE 10-5**

**Enabling Intrusion Detection**

1. Click Start | Programs | Microsoft ISA Server.
2. In the ISA Server Management tool, expand Servers and Arrays, then expand the desired array.
4. Right-click IP Packet Filters, then click Properties.
5. On the General tab, verify that packet filtering is enabled, then click the Enable Intrusion Detection check box.

6. Click the Intrusion Detection tab, shown in Figure 10-10. Click the check boxes to enable the intrusion methods that you want to detect. If you want to detect port scans, enter the desired values. The default setting is 10 well-known port scans and 20 port scans. These settings are typically all you need. Click OK when you're done.

---

**FIGURE 10-10**

Intrusion Detection tab
Is other intrusion detection software available? There are a number of companies who make intrusion detection software, some of which can be used in conjunction with Microsoft ISA Server. In the future, you can also expect to find third-party applications and utilities that are specifically designed to work with ISA Server.

Can I use intrusion detection without using packet filtering? No. The intrusion detection software found in ISA Server functions at the packet level, so packet filtering must be enabled or the option to enable intrusion detection will be grayed out.
Creating and Managing Routing Rules

ISA Server can be used to route Web requests as needed for your network. When routing is used with packet filtering, you maintain network security, but gain the advantage of having ISA Server act as a router. This feature enables you to use a DMZ configuration, chained ISA configurations, and even determine how client requests are retrieved from certain locations. In short, the routing option provides you with a number of helpful features so that ISA Server can meet your networking needs.

You can create new routing rules as needed, but there is a default rule that is found by expanding the desired server, expanding Network Configuration, and expanding Routing. You see the default rule listed in the right pane. This rule can be edited, but not deleted, and it simply tells ISA Server to retrieve all Internet requests from the specified destination. In other words, there is no routing intervention that redirects requests. If you have no specific routing needs, then this default rule will be the only one you need.

If you need to create a routing rule, the rules are ordered in the number that you create them, with the default rule always being last. For example, if you create a new rule, it will be rule 1 with the default rule being last. If you create another rule, it will become rule 1, with the previous rule becoming rule 2, and the default rule remaining last. When a client request is made, ISA Server checks the routing rules, looking at each rule in order until a match for that particular request is made, or the default last rule is simply applied.

It is important to note here that routing rules and management can also be made using Routing and Remote Access (RRAS) in Windows 2000. RRAS also allows you to use dial-up connection with ISA Server. These options will be explored in Chapter 14.

Routing rules can also provide bridging functions. Bridging allows ISA Server to repackage requests and transmit them using secure standards. For example, you want all HTTP requests received at a particular server to be routed to an upstream server.
across a nonsecure link. You could have all of those requests be rerouted at SSL requests to the receiving array for security purposes. In the same manner, when a client makes a request to the Internet using SSL, ISA Server can terminate the SSL transmission, and repackage it as a different SSL transmission. This security feature allows no direct SSL tunnel to hit the Internet from a client computer. Aside from bridging, ISA Server also provides SSL tunneling, where the same SSL connection is used with the client and the Web server, but is simply tunneled through ISA Server.

Before looking at Exercise 10-6, let’s consider an example of how a routing rule might be used. Routing rules apply to destination sets that can be configured for either incoming or outgoing access. For example, your primary network is located in Dallas, but you have a smaller office in Tulsa. You want all HTTP requests made to the ISA Server to be routed to the Dallas array rather than directly retrieving those requests from the Internet. You can configure all HTTP requests to be redirected as HTTP requests and SSL requests to be redirected as SSL requests, depending on your needs.

**EXERCISE 10-6**

**Creating a Routing Rule**

Create a routing rule by following these steps:

1. Click Start | Programs | Microsoft ISA Server.
2. In the ISA Server Management tool, expand Servers and Arrays, then expand the desired array.
3. Expand Network Configuration.
4. Right-click Routing, then click New | Rule.
5. The New Routing Rule wizard appears. Enter a name for the rule, then click Next.
6. In the Destination Sets window, click the drop-down menu to select a desired destination set, then click Next.
7. In the Request Action window, shown in Figure 10-11, you can choose to retrieve requests directly from the Internet, route them to an upstream server,
or redirect them to a hosted site. You can also choose to use a dial-up entry by clicking the check box. Make your selection and click Next.

8. If you choose to route to an upstream server, the Primary Routing window appears so you can select which server that you want to route upstream to. Enter the account information and click Next.

9. In the Backup Routing window (which only appears if you chose to route to an upstream server), choose the action that should be taken if the primary route is not available. You can ignore the requests, retrieve them directly from the Internet, or route to a different upstream server. Make your selection and click Next.

10. The Cache Retrieval Configuration window appears, as shown in Figure 10-12. Click one of the radio buttons to select a cache retrieval method to determine how the rule searches the cache before routing the request. The default option is to use a valid cached object if one exists. Make your selection and click Next.
11. The Cache Content Configuration window appears. There are three radio button options that determine how content is cached that is retrieved from the routing rule. Your options are to cache all content, cache only content that contains cacheable source and header content, or never cache content. The second option is selected by default. Make your selection and click Next.

12. Click Finish to save the rule.

Once the rule is created, it will appear in the Routing folder under Network Configuration. If you access this folder, you will see the rule listed in the right window. By double-clicking the rule, you can make configuration changes to it.

I do want to call your attention to the Bridging tab, shown in Figure 10-13. As you can see, you can make changes to the default options in order to configure any bridging needs you might have. By default, HTTP request are redirected as HTTP requests and SSL requests are redirected as SSL requests. You can also choose to enforce SSL communicate and provide a certificate for the SSL Web server. Under
normal circumstances, the default options are all you need, but in highly secure environments, the SSL options may be used.

**CERTIFICATION SUMMARY**

This chapter explored packet filtering and routing and intrusion detection. ISA Server provides a multi-layered firewall by providing protection at various levels of IP communication. The lowest level of protection is at the IP packet level. ISA Server can dynamically open and close ports and allow or deny IP traffic at the packet filtering level once packet filtering is enabled. Although the primary method of configuring security is through policy and rules, you can also create static packet filters to meet particular application or networking needs, such as in the case of a custom application or a DMZ network configuration. Packet filtering can be enforced at the enterprise level through policy, or at the array level.
ISA also provides another level of security with intrusion detection which can recognize various Denial of Service attacks and trigger alerts that you configure. Intrusion detection functions at the IP packet level and is only functional if packet filtering is enabled.

Routing rules can be configured so that ISA Server can route desired requests to other destinations, such as in the case of DMZ network chain configurations. When routing is enabled, packet filtering should also be enabled or ISA Server will simply act as a router, allowing all information into the network. Routing rules provide you an effective way to meet specialized networking needs.
TWO-MINUTE DRILL

Understanding Packet Filtering and Routing

- Packet filtering denies all packets once it is enabled. Through site and content and protocol rules, IP ports can be dynamically opened and closed to allow packets based on the rule. Packet filtering is considered a part of Access Policy.
- Packet filtering can be enforced on all arrays through enterprise policy, or it can be applied at each individual array.
- Packet filters can either be dynamic or static. Dynamic packet filters are created via policy and they dynamically open and close IP ports as needed. Static filters are created with a wizard and can be used for specialized needs.
- Routing should not be enabled without packet filtering. This is considered a security breach and basically turns ISA Server into a router.

Creating and managing packet filters

- Packet filtering is enabled by accessing the IP Packet Filters folder properties.
- Static packet filters are created in the ISA Management console via a wizard.
- Using the IP Packet Filters folder, you can also choose to filter IP fragments, packets with IP options, and to log packets from Allow filters.
- Packet filters for DMZ networks are created statically with the New Packet Filter wizard.

Configuring Intrusion Detection

- ISA Server provides intrusion detection software for Denial of Service attacks.
- The DoS attacks detected are WinNuke, landattack, ping of death, IP half scan, UDP bomb, and port scan.
- Intrusion detection can be easily enabled on the IP Packet Filters Properties pages, but can only function if packet filtering is enabled.
Creating and Managing Routing Rules

- Routing rules provide a way to configure a number of routing options specific for your network needs.
- Routing rules can be used to route both inbound and outbound requests to specific upstream servers or Web servers as well as direct connections.
- Routing rules support bridging features where HTTP and SSL requests can be repacked and routed to an appropriate server.
SELF TEST

The following questions will help you measure your understanding of the material presented in this chapter. Read all of the choices carefully, as there may be more than one correct answer. Choose all correct answers for each question.

Understanding Packet Filtering and Routing

1. What items are collectively considered “access policy?” (Choose all that apply.)
   A. Bandwidth rules
   B. Site and content rules
   C. Packet filters
   D. Enterprise policy
   E. Protocol rules

2. At what two levels can packet filtering be enabled? (Choose two.)
   A. Enterprise policy level
   B. Array policy level
   C. Site and content rule level
   D. Protocol rule level
   E. Application level

3. Which statement best describes the default packet filtering setting?
   A. All HTTP packets are allowed.
   B. All HTTP packets are denied.
   C. All IP packets are allowed.
   D. All IP packets are denied.

4. You create a static packet filter using the ISA Management console. Which statement is true about this filter?
   A. The static filter can dynamically open the IP port as needed.
   B. The static filter opens the IP port – it cannot be dynamically closed and reopened.
   C. The static filter copies the configuration of a dynamic filter.
   D. The static filter resides outside of policy scope.
5. An administrator on a particular network enables routing on an array without packet filtering. What is the result?
   A. All IP packets are blocked at the firewall.
   B. All IP packets are routed through the firewall.
   C. All IP packets are processed according to rules.
   D. There is no result.

6. Which statement best describes how ISA Server packet filtering works?
   A. A single filter inspects all IP traffic.
   B. A single filter listens on various IP ports as configured.
   C. Multiple filters inspect all IP traffic on a single port.
   D. Multiple filters listen on various IP ports as configured.

Creating and Managing Packet Filtering

7. Consider the following window from the ISA Management console, shown in Figure 10-14. Which of the following statements is true?
   A. Packet filtering is forced on every array.
   B. Packet filtering is forced on a particular array.
   C. Packet filtering is available on every array.
   D. Packet filtering is available on a particular array.
8. As an administrator, you inspect the IP Packet Filters Properties window, as shown in Figure 10-15.

You notice that the packet filtering option is enabled and grayed out. What is causing this configuration?

A. An enterprise policy is enforcing the configuration.
B. An array policy is enforcing the configuration.
C. ISA Server is installed as a dedicated firewall.
D. Caching functions force packet filtering on the array.
9. To increase network protection, you enable the filtering of IP fragments so that no fragmented IP packets are allowed to pass through the firewall. However, your environment uses streaming media, and now no streaming media is being allowed into the firewall. What do you need to do?

A. Create a protocol rule for streaming media
B. Create a content rule that allows streaming media.
C. Create a static packet filter for streaming media.
D. Enable IP fragments to pass through the firewall.

10. You need to create a static packet filter that allows a certain protocol to pass through the firewall for a custom application you are using. You have an array of ten ISA Servers. Only 200 network clients use the custom application, and only then on a sporadic basis. You do not want to enable this static filter on the entire array, yet these 200 clients do need to use this application from time to time. What solution should you consider?

A. Apply the static filter to the entire array on a timed basis.
B. Configure a stand-alone ISA Server to handle the static filter.
C. Apply the filter to a single array member, then direct the clients to contact that ISA Server for service.
D. You have no option but to apply the filter to the entire array.

11. You want to create a static packet filter so that SMTP traffic is sent to an SMTP server in a DMZ. What actions do you need to take to create this configuration? (Choose all that apply.)

A. Ensure that the DMZ IP address range is not listed in the LAT.
B. Ensure that the DMZ IP address range is listed in the LAT.
C. Create a packet filter that allows traffic for the SMTP protocol and routes it to the IP address of the server in the DMZ.
D. Create a packet filter that denies traffic for the SMTP protocol and routes it to the IP address of the server in the DMZ.
E. Create a dynamic packet filter through a protocol rule that allows SMTP and transfers the traffic to the DMZ server.
F. Enable packet filter on the desired array.
G. Enable routing on the desired array.
H. Disable routing on the desired array.

12. You have created a static packet filter on a certain array. The reason for this static filter is so that a particular server on the Internet can send application-specific IP traffic to a particular
server on your local network. In other words, this packet filter exists to meet the communication needs of a server on your local network and a single server on the Internet. However, you know that a static filter keeps the port open at all time and you are concerned that Internet intruders might compromise this port. Which option should you choose to provide an additional measure of security?

A. Add the remote computer to the LAT.
B. Configure the filter to only send traffic on this port to the desired internal server.
C. Configure the filter to only accept traffic from the remote server.
D. You cannot provide any additional security in this scenario.

Configuring Intrusion Detection

13. You want to use ISA Server’s intrusion detection software on a certain array. However, the option is not available. What must you do before you can use intrusion detection?

A. Configure a routing rule.
B. Enable packet filtering.
C. Force intrusion detection at the enterprise policy level.
D. Force intrusion detection at the IP packet level.

14. You want to make certain that your network is protected from Internet attacks that use ICMP echo floods that can cause a buffer overflow. What type of attack do you want to prevent?

A. Land attack
B. Ping of death
C. IP half scan
D. Port scan

15. You want to make certain that your network is protected from Internet attacks that use an RST packet in a response instead of an ACK packet. What type of attack do you want to prevent?

A. UDP bomb
B. Land attack
C. IP half scan
D. WinNuke
Chapter 10: Configuring Packet Filtering and Routing Rules

Creating and Managing Routing Rules

16. Which statements are true concerning the default routing rule? (Choose all that apply.)
   A. You can edit the default routing rule.
   B. You cannot edit the default routing rule.
   C. You can delete the default routing rule.
   D. You cannot delete the default routing rule.
   E. The default routing rule is always last.
   F. The default routing rule is always first.

17. Consider the list of routing rules, shown in Figure 10-16.
   From looking at the rule list, what will happen when an internal client makes a service request to the ISA Server?
   A. The request will be directly serviced.
   B. The request will be sent to a Web server.
   C. The request will be routed to a specified destination.
   D. The request will be refused.

18. Consider the list of routing rules, shown in Figure 10-17.
   You have a client address set called “Web Server.” Requests from this client address set should be directly retrieved from the Internet. By looking at the rule list, what action will occur for the Web Server client address set?
   A. The request will be directly retrieved.
   B. The request will be routed.
   C. The request will be routed to an alternate destination.
   D. None of these actions will occur.

<table>
<thead>
<tr>
<th>Figure 10-16</th>
<th>Dider</th>
<th>Name</th>
<th>Action</th>
<th>Cache</th>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routing Rules</td>
<td>1 Subnet</td>
<td>Route to alternate destination</td>
<td>Connect if valid obj.</td>
<td>All external destinations</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2 Chan</td>
<td>Route</td>
<td>Connect if valid obj.</td>
<td>Web Server</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Last Default rule</td>
<td>Retrieve the request directly</td>
<td>Connect if valid obj.</td>
<td>All destinations</td>
<td></td>
</tr>
</tbody>
</table>
19. What routing feature of ISA Server allows the server to repackage client requests and transmit them using secure standards?
   A. Caching
   B. Linking
   C. Tunneling
   D. Bridging

20. What routing feature allows ISA to provide a passthrough mechanism for SSL requests?
   A. Caching
   B. Linking
   C. Tunneling
   D. Bridging

**LAB QUESTION**

Using the ISA Server Management tool, create a packet filter that has the following parameters:

- The filter should apply to all computers in the array.
- The filter should allow the POP3 protocol to be allowed.
- The filter should send all POP3 packets to a computer on a DMZ network that has an IP address of 10.0.0.2.
- Apply the packet to a remote computer with an IP address of 131.107.2.17.
SELF-TEST ANSWERS

Understanding Packet Filtering and Routing

1. B, C, and E are correct. Site and content rules, protocol rules, and packet filtering are considered the three portions of access policy. Access policy collectively defines what sites, content, and protocols your users are allowed to access. Packet filters are also used to enforce access policy at the packet level.
   A and D are incorrect. Enterprise policy, which drives access policy, is not actually considered a part of the policy. Also, bandwidth rules are not considered a part of access policy.

2. A and B are correct. Packet filtering can either be enabled at the enterprise policy level, where packet filtering is enforced on all arrays in the enterprise, or it can be enabled at the array level where you can use packet filtering on individual arrays as needed.
   C, D, and E are incorrect. Packet filtering is enabled by either enterprise or array level policy, so none of these options is correct.

3. D is correct. By default, all IP packets are denied access when packet filtering is enabled. You can then create protocol rules that will create “allow” packet filters to allow the desired traffic.
   A, B, and C are incorrect. Since all IP traffic is denied by default, none of these options is correct.

4. B is correct. A static filter opens an IP port – it cannot dynamically open and close that port. This is why dynamic packet filters, created through protocol rules and site and content rules, are always more favorable than static packet filters.
   A, C, and D are incorrect. Static filters cannot dynamically open ports. Also, static filters do not copy configuration information or fall outside of the policy scope.

5. B is correct. If you enable routing without packet filtering, ISA Server simply acts as a router and passes all IP traffic to the internal network. This is considered a security breach and is not a recommended use of ISA Server.
   A, C, and D are incorrect. The router passes all IP traffic, regardless of any rules. Since packet filtering is not enabled, no IP traffic is blocked at the firewall.

6. D is correct. Packet filtering closes all ports by using “deny” filters. These filters do not listen on any IP ports for incoming requests. With your rules and policies, “allow” filters are created that allow IP traffic through various ports. These filters listen to those ports for access requests.
A, B, and C are incorrect. Multiple filters are used, so answers A and B are incorrect. Also, multiple ports are listened to, so answer C is incorrect.

Creating and Managing Packet Filtering

7. ✓ A is correct. The Set Defaults window provides the default settings for the entire enterprise, so judging from these settings, you can determine that packet filtering is enforced on every array according to the enterprise defaults.
   ✗ B, C, and D are incorrect. This window applies to the entire enterprise, so we know that the packet filtering enforcement does not apply to a single array. Also, with this setting, packet filtering is not optional at the array level – it is enforced.

8. ✓ A is correct. The enterprise policy is forcing packet filtering on all arrays. When the policy forces packet filtering, packet filtering is enabled and the option to disable it is grayed out.
   ✗ B, C, and D are incorrect. Array level policies will not create a forced configuration. Firewall or caching settings will not force packet filtering on the array – this is only done by an enterprise policy setting.

9. ✓ D is correct. IP fragment filtering provides an additional measure of protection because some malicious attacks use IP fragments that can reassembled once they enter the firewall. However, if you use streaming media, you cannot use the IP fragment filtering option because the filter will see streaming media as fragmented packets.
   ✗ A, B, and C are incorrect. You can’t use any additional rules or static filters to enable streaming media if IP fragment filtering is in use. The only solution is to simply not use IP fragment filtering in order to allow streaming media to function.

10. ✓ C is correct. The IP Packet Filter wizard gives you the option to apply a static filter to an entire array or an individual server in the array. Using this option, you can direct clients who use the custom application to contact the array member for service. This way, you use the needed filter, but you keep the number of static ports that are open to a minimum.
    ✗ A, B, and D are incorrect. You can’t configure packet filters on a “timed” basis, and configuring a stand-alone server is completely unnecessary. Since you can apply a filter to a single array member, this is the best choice in this situation.

11. ✓ A, C, F, and G are correct. In order to create a packet filtering configuration for a DMZ server, you first need to ensure that the IP address range for the DMZ is not listed in the LAT. Listing the DMZ range in the LAT is a security breach. Next, enable packet filtering and routing on the desired array. Then, create a packet filter for the desired protocol and use the New IP Packet wizard to configure the ISA Server to forward the traffic to the server in the DMZ network.
**Chapter 10: Configuring Packet Filtering and Routing Rules**

B, D, E, and H are incorrect. You would not want to list the DMZ IP address ranges in the LAT, so B is incorrect. You would not want to deny the traffic that you want to divert to the DMZ, so D is also incorrect. You cannot create a dynamic packet filter to reroute packets to the DMZ. This must be done by creating a static packet filter. Finally, if you disable routing on the array, the packet filter cannot be routed to the DMZ.

12. ✔ C is correct. In a situation where one computer or a group of computers will be communicating with a particular port, you can configure the packet filter that manages that port to only accept traffic from that IP address or IP address range. This configuration gives you an extra measure of protection. You can configure this option during the creation of the packet filter with the IP Packet Filter wizard, or afterwards by accessing the filter’s properties sheets.

A, B, and D are incorrect. Adding the remote computer to the LAT would be a security breach, not a way to increase security. Configuring the filter to pass all traffic to the certain internal server will not provide any additional security. The best security feature you can invoke here is the restricting of remote computers that can send data to the port.

**Configuring Intrusion Detection**

13. ✔ B is correct. Intrusion detection works at the IP packet level, so for the intrusion detection option to be available, packet filtering must be enabled on the array.

A, C, and D are incorrect. Routing rules will not enable intrusion detection. It is not enabled by forcing it through enterprise or array level policies.

14. ✔ B is correct. The ping of death uses ICMP echo pings to overflow a buffer, causing the computer to crash.

A, C, and D are incorrect. These attacks do not use ICMP echo pings.

15. ✔ C is correct. The IP half scan attack issues an RST packet instead of an ACK packet during a TCP session. The RST packet can be used to probe the port and gain information while the computer is waiting for the ACK packet.

A, B, and D are incorrect. These attacks do not use an RST packet.

**Creating and Managing Routing Rules**

16. ✔ A, D, and E are correct. The default routing rule can be edited, but not deleted, and the default routing rule is always last in the rule list.

B, C, and F are incorrect. Each of these statements is the opposite of what is true about the default routing rule.
17. ✓ C is correct. Looking at the rule list, you can see that an action is applied to all external destinations, which is to route the request to a specified alternative destination.
   ✗ A, B, and D are incorrect. These actions do not match the provided rules given for a user requesting access to an Internet site (external destination).

18. ✓ B is correct. It is important to remember that routing rules are ordered and applied in order. Notice that rule 2 routes all external destinations. Although rule 3 retrieves the requests directly for the Web Server address set, the 2nd rule will be applied first, so the requests will still be routed. In order to fix this problem, move rule 3 so that it is positioned before the current rule 2.
   ✗ A, C, and D are incorrect. The rule order will not allow any of these actions to occur.

19. ✓ D is correct. Bridging is a function where ISA Server can repackage a user’s request into an SSL request, or vice versa, as needed or desired for network communication.
   ✗ A, B, and C are incorrect. None of these terms define ISA’s secure repackaging feature.

20. ✓ C is correct. SSL tunneling allows ISA Server to tunnel SSL requests between a client and server without interacting in the authentication process.
   ✗ A, B, and C are incorrect. None of these terms define ISA’s SSL tunnel features.

**LAB ANSWER**

To configure a packet filter with the requested parameters, follow these steps:

1. Click Start | Programs | Microsoft ISA Server.
2. In the ISA Server Management tool, expand Servers and Arrays, then expand the desired array.
4. Right-click IP Packet Filters, then click New | Filter.
5. The New IP Packet Filter wizard appears. Enter a name for the filter, then click the Next button.
6. The Servers window asks you if the filter should apply to all servers in the array or on this individual server. Apply the filter to the array, and then click Next.
7. The Filter Mode window appears. Click the desired radio button to either allow or block packet transmission. Click the Allow radio button, and then click Next.
8. The Filter Type window appears. Choose the predefined filter option, and then use the drop-down menu to the POP3 filter. Click Next.

9. The Local Computer window appears. Choose to apply the filter to a computer on a perimeter network. Enter the IP address of 10.0.0.2 and click Next.

10. The Remote Computers window appears. Choose the remote computer option and enter an IP address of 131.107.2.17.

11. Click Finish to save the static filter.