Routers, Firewalls, and the Internet: Section 1 Transcript

Introduction

Welcome to the Routers, Firewalls, and the Internet module. By now you should understand simple packet traversal as it moves through the network; however, modern networks include a variety of transparent complex filtering, proxy, and translation mechanisms that affect how your packet actually flows, and how and whether it actually gets to its intended destination. Within this module we will discuss the roles of core network components as the gates of network traffic, and their inherent handles and locks used for filtering packets to the desired route and destination.

Throughout this module, you'll be presented with opportunities to assess and apply what you've learned.

At the end of this module, you will be able to:

- Describe Internet Protocol (IP) network filtering devices,
- Describe Autonomous Systems (AS),
- Identify how Regional Internet Registries (RIR) relate to AS Numbers,
- Explain IP Network Address Translation (NAT),
- Explain IP Network Address Port Translation (NAPT),
- Recognize the differences between various firewall types, and
- Translate router configurations for network communication.

Bypass Exam Introduction

If you are already familiar with the subject matter presented in this module, you can choose to take a Bypass Exam to skip this module.

The Bypass Exam option provides a single opportunity to successfully demonstrate your competence with the material presented within the module. If you pass, you'll receive credit for completing the module, unlocking the content within, and you will be free to proceed to the next module. If you do not pass, you will need to successfully complete the module, including all exercises and the Module Exam, to receive credit.

Click the Next Section button to continue.

Routers, Firewalls, and the Internet: Section 2 Transcript

IP Network Filtering Devices

Network filtering devices typically involve three core network components: routers, firewalls, and switches. These network devices are the invisible gates that control access to and from internal and external resources. The handles and locks on these gates come in varying shapes and sizes and include network traversal tools. Some of these tools include:

- Routing tables,
- Stateful, stateless, and application proxy firewall configurations,
- Access Control Lists (or ACL),
- Network Address Translation (NAT), and
- Network Address Port Translation (NAPT).

We will go over all of these tools, but first let's discuss one of the major components of IP filtering to and from the Internet, Autonomous Systems, or AS.

Autonomous Systems

Typically, an Autonomous System, or AS, is a group of network devices, for example routers and switches, that are administered under a single technical administration. That could be one common company, organization, or divisions of an organization. They possess a clearly-defined routing policy to the Internet.

Organizations that route public IP addresses receive Autonomous System Numbers (ASNs). ASNs are used to uniquely identify networks on the Internet.

The routing protocols that are used inside an AS are called Interior Gateway Protocols (IGPs), and those used to exchange routes between AS's are called Exterior Gateway Protocols (EGPs). Nowadays, the Border Gateway Protocol (BGP) is the only EGP in use.

Border Gateway Protocol

BGP, a path vector protocol, is the core routing protocol used on the Internet. Path vector protocols only store the next-hop router address, not a complete picture of the network. They exchange information about the path to the destination network. Two BGP peers connect to each other and form a TCP session. BGP then advertises available routing paths that network traffic can take to access other IP addresses between ASNs. The BGP tables select, and advertise the best routes for the network traffic. Those tables often provide superior insight into IP traffic ownership, when compared to the physical or the logical layer. They are useful in understanding the evolution of public-facing ASNs and IP filtering at a high level. BGP routing tables reveal administrative ownership, organizational-peering relationships, and data paths through physical connections.

For more information on various protocols, please refer to Resources.

Weird Connections, Routes, and Detours

There are different scenarios that could occur and cause nonsensical connections, routes, and detours. Three of those scenarios include IP hijacking, IP leasing, and organizational Service-Level Agreements, or SLAs. Let's look at IP hijacking first.

IP Hijacking

There are times when individuals or entities broadcast, either intentionally or unintentionally, erroneous paths to access a particular public IP address on the Internet. Data reaches its intended destination after the suspicious detour, so this is often overlooked and users are oblivious. IP hijacking is the intentional illegitimate route advertising and takeover of groups of IP address by corrupting Internet routing tables. This is also sometimes referred to as BGP hijacking, prefix hijacking, or route hijacking.

When one group advertises incorrect routing information, routers across the globe can be convinced to send traffic on geographically ridiculous paths. On April 8, 2010, China infamously swallowed 15% of all Internet traffic for 18 minutes. According to the US-China Economic and Security Review Commission's 2010 Report to Congress:

For about 18 minutes on April 8, 2010, China Telecom advertised erroneous network traffic routes that instructed U.S. and other foreign Internet traffic to travel through Chinese servers. Other servers around the world quickly adopted these paths, routing all traffic to about 15 percent of the Internet's destinations through servers located in China. This incident affected traffic to and from U.S. government (.gov) and military (.mil) sites, including those for the Senate, the Army, the Navy, the Marine Corps, the Air Force, the Office of Secretary of Defense, the National Aeronautics and Space Administration, the Department of Commerce, the National Oceanic and Atmospheric Administration, and many others. Certain commercial websites were also affected, such as those for Dell, Yahoo!, Microsoft, and IBM.

This case is described on page 244 of the report, which can be found in Resources.

Regional Internet Registries

Several methods exist to reveal ridiculous IP paths and attributing information on Internet entities. Regional Internet Registries (RIR) allocate IP addresses and assigns ASNs to various organizations for different regions of the world. RIRs are broken down into five regions across the globe.

- The African Network Information Centre (AFRINIC) is responsible for the continent of Africa,
- The American Registry for Internet Numbers (ARIN) is responsible for the United States, Canada, several parts of the Caribbean, and Antarctica,
- The Asia-Pacific Network Information Centre (APNIC) is responsible for Asia, Australia, New Zealand, and neighboring countries,
- The Latin America and Caribbean Network Information Centre (LACNIC) is responsible for Latin America and parts of the Caribbean, and
- The Réseaux IP Européens Network Coordination Centre (RIPE NCC) is responsible for

Europe, Russia, the Middle East, and Central Asia.

IP Leasing

Sometimes individuals or organizations advertise an IP address that they do not own. This is typically done if an individual or organization does not want a large block of IP addresses. They instead can talk with the IP owner, whether that is an Internet service provider (ISP) or a company that does not need all their currently-owned IP addresses. Relationships exist between the actual IP owner and these individuals or organizations; however, publicly available confirmation of this relationship may or may not exist. This relationship can be discerned through routes that network traffic follows, as advertised through BGP routing tables. We will discuss routing tables later in this module. Let's see an example of this in action.

The Inspector Possum company recently launched a new baby-friendly fertilizer that was hailed as the safest fertilizer in the world by Better Fertilizer Magazine. Because of their success, they signed a lease with their ISP in order to have a static IP address. Inspector Possum wanted to lease the IP address because, if the address was dynamic, each time the router resets, their server and email could become unreachable by the thousands of fertilizer enthusiasts looking for their product.

Although leasing IP addresses is completely legal, as long as the leaser owns the IP address, there is a black market where hacked IP addresses are illegally leased.

Organizational Service Level Agreements (SLA)

In addition to IP hijacking and IP leasing, organizational Service Level Agreements, or SLAs, are another way of implementing path control. Let's see how SLAs work.

The RAD Turtle company owns IP space located in a data center that they want to be easily reachable by their target audience and has two paths: 10.1.1.1 and 172.22.2.2. As a result, The RAD Turtle advertises the same IP space from multiple locations, along with the ASNs associated with them. Although they maintain vast IP space, The RAD Turtle only has two ASNs: one in the United States and one in France. While the company advertises IP addresses through either ASN, network traffic is directed to the closest one.

Routers

Routers are devices or machines with interfaces on multiple networks that are responsible for routing packets between networks. Routers form the backbone of networks, along with hubs and switches, and are usually dedicated hardware loaded with some form of firmware. Some vendors of dedicated hardware router products are Cisco, Juniper, Huawei, and Vyatta. Because Cisco has a large market share, we will focus on configurations for their products.

Routing focuses on the logic required to deliver packets end-to-end. This logic is determined by routing metrics that describe route efficiency. Data is exchanged between network routers using different routing protocols to dynamically determine the most advantageous route for packets to take.

Routers are required to know how to reach remote networks in order to forward packets to them. This can be done by manual configuration, known as a static route, or by using a routing protocol to

exchange information about network reachability. These routing protocols discover neighboring routers and attached networks. This allows routers to exchange information about the network topology as it changes, when new links are created, or when links are no longer valid.

Another special type of route is known as a default route. A default route in IPv4 is designated by 0.0.0.0 with a subnet mask of 0.0.0.0. A default route in IPv6 is designated by ::/0. Default routes are used when no other route exists to the destination network.

The Routing Table

Routers maintain routing tables, which are databases of routes they use when forwarding packets. When routers automatically build the routing tables, it rules out invalid routes. They know a route is valid or invalid when it attempts to verify hops. If the sent data does not get to its destination, it is an invalid route. Let's explore the steps a router uses to find a valid path when using dynamic routing tables.

- First, for each route received, verify the next hop. If it is invalid, the router discards the route.
- And then, if multiple identical valid routes are received by a routing protocol, the router chooses the lowest metric based on the Administrative Distance (AD). Routes are identical if they advertise the same prefix and mask; therefore, 172.16.0.0/16 and 172.16.0.0/24 are separate paths and may each be placed into the routing table.
- Finally, if the same valid route is advertised by different routing protocols, choose the path with the lowest AD.

Choosing the Route

After the routing table is built, routers choose which route to use for a specific packet by looking for a match to the destination IP address. The route will rarely match the destination IP address exactly, so the router looks for the longest match.

Let's say that Steve from Accounting sends a packet that is bound for IP address 10.1.1.1. The routing table has a route for 10.1.0.0/16, one for 10.1.1.0/24, and a default route of 0.0.0.0. The default route matches 0 bits of the destination address; the 10.1.0.0 route matches 16 bits of the destination address; and the 10.1.1.0 route matches 24 bits of the destination address. The 10.1.1.0 route is the longest match, so it will be used to forward the packet.

Refer to this module's Resources for additional information on Classless Inter-Domain Routing (CIDR), which explains how we know how many bits of the destination address match the designated routes.

Router Filters

Filtering is used to detect and block unauthorized or undesired traffic between networks. This is done in order to block packets that are known to be vulnerable or malicious, or to limit Internet access for specified nodes. Imagine there are ten workstations, but you only want two of them to have Internet accessibility. Using filters, you can prevent the other eight computers from having access.

Route filters can be manually or naturally applied. Manual filters, are filters that have been set up manually on routers, i.e., the router has been manually told who the router can talk to.

Naturally applied filters are filters that have been automatically assigned by the router. This form of assigning filters is typically used when conducting input and output filtering.

- Input filtering is applied when a filter is affixed to routes as they learn from a neighbor. A neighbor refers to another router next to it, from a logical standpoint. If filtered out, it is discarded and not considered for inclusion in the local routing database.
- Output filtering is applied before announcing routes to a neighbor. If filtered out, the neighbor never learns about the route and it is not considered for inclusion in the local routing database.

Section Completed

Routers, Firewalls, and the Internet: Section 3 Transcript

Cisco Router Introduction

We will cover TCP/IP networking in an Internet environment, through Cisco router configurations; however, Cisco specializes in many other technologies and features. This information is designed to give you a general overview of Cisco Internetwork Operating System (IOS) software router configurations, and some tips for performing live surveys. We are going to focus on the Cisco router command line, which gives you complete control over every facet of router behavior. For more in-depth information, Cisco does a great job at making their data available, as long as you know what you are looking for. One of the best routes to find this information is through Google search engine.

Now, let's start with some commands and concepts for familiarization, along with some configuration snippets, because a complete configuration printout can be hundreds of lines long.

Cisco Router Configuration

By default, when you log in to a Cisco router, you are in EXEC mode. You can execute diagnostic commands, but you cannot change configuration settings or view sensitive details. For example, you can ping across a circuit to see if it is working, but you cannot reset the interface. In EXEC mode, the command prompt ends in a greater than sign.

In order to make changes, or to run more invasive commands, you need to be in privileged EXEC mode, which is the administrator security level protected by a unique password. This administrator mode is also known as enable mode. Within enable mode, you can configure the router in any way desired. You can reboot the system or take any other software action. To enter privileged EXEC mode, you have to use the enable command. Once in this mode, the command prompt ends in a pound sign.

Administrators can also create discrete individual usernames with privileges set; however, the norm for technicians especially in a small organization is to use only unprivileged, or EXEC mode, and privileged, or enable mode, accounts.

Hints

Once you log in, an entry of a single question mark at the command prompt displays the available commands. Additionally, you can request hints for specific commands, syntax, and the features available at that privilege level by typing the command and a question mark. For example, if you want to know what arguments the show command can take, enter `show ?`.

Hints on particular commands are only available in the mode that the command is available. Entering a privileged command in standard EXEC mode generates an unrecognized command error. For example, look at the difference in the features available via the show command in EXEC

mode, as compared to privileged EXEC mode.

Command Search Abbreviation

You can abbreviate command names to the shortest abbreviation of a word when searching for commands; however, it's important to remember that Cisco makes some abbreviations, such as `sh` for `show`, equivalent to their command when entered.

Let's search for commands that begin with the letter s, by entering `s?`. For the EXEC output we get two commands, `show` and `ssh`. Now, let's enable privilege EXEC mode, and try that again. This time it prints three commands, `setup`, `show`, and `ssh`.

Show Version

The `show version` command explains some basic facts about a router. It includes details such as:

- Supported interfaces,
- Hardware type,
- Software type,
- Software version,
- Feature set, and the
- Amount of system memory.

The format, as well as an example from Cisco, is supplied in Table X and X1, which can be found in the Resources tab. Next, we will be discussing this information, so we recommend you have that resource open as a reference.

X1 Table Highlights

In table X1, we can learn quite a bit about the target router. In the first line, the table gives us the version number and the hardware platform that the IOS uses. We also can discern who built this software, and when it was built.

Next, we can determine the ROM version and the router uptime. The uptime displays how long the router has been running, in weeks, days, hours, and minutes. The next line describes why the router last went down. According to the table, it went down because of a reload, which is a software-driven reboot. The system image file is the location and name of the file that the router has loaded as its operating system.

This section of the table lists the model information and physical characteristics of the router.

X1 Table Highlights

After a few more lines that detail software features, you will see:

- The interface types installed,
- A list of model descriptions for components, and

- The configuration register.

The configuration register is a hex value that shows the current value of the software configuration register; however at the next reload, the value displayed in parenthesis will be used. The final digit (boot field) of the software configuration register dictates what the system does after a reset. For example, if the boot field is set to 0x1, the system automatically boots the first Cisco IOS image found in the onboard Flash memory. The factory-default setting for the configuration register is 0x2102. This value indicates that the router will attempt to load a Cisco IOS software image from Flash memory and load the startup configuration file.

Cisco Configuration

At any given time, a router has two configurations: the startup configuration and the running configuration. The startup configuration is stored in the router's NVRAM (non-volatile memory). At boot, the router loads the startup configuration as the current configuration, and a copy of the startup configuration becomes the running configuration. If you change the router's configuration while running, you are only changing the running configuration. When saving the running configuration, it overwrites and becomes the new startup configuration. If you do not save your changes before the router reboots, your changes will be lost.

Cisco Configuration

To configure a router, you must be in privileged EXEC mode. Once in EXEC mode, enter configure mode with the configuration terminal command prompt, `conf t`. When you enter this mode, or any other mode, you will notice a change from `router` to `router(mode)`. Commands appear exactly like those in system configuration and are added to the router configuration, creating an appropriate spot in the global configuration. To configure a particular interface, enter the interface name at the prompt. Remember that you can enable and disable features and protocols on a per-interface basis. In this mode, you see the config mode subprompt updated with a `-if` statement. Routing protocols, like all subprompts, can be entered just like the main prompt. To exit the subprompt, enter `exit`. To exit a mode, use CTRL-Z to return to the basic router.

Only legitimate configuration statements are accepted. An error will show for incorrect statements. When an erroneous command is entered, the invalid input is isolated and indicated in the form of a caret symbol. The caret appears at the point in the command string where the incorrect or unrecognized command syntax is found.

Entering configuration statements update and alter the running configuration; however, this does not persist after a reboot, unless it is saved. This can be done with the command, `copy running-config startup-config`, or `write memory`, or `wr mem`.

Cisco Configuration

On most routers, a field of 30 characters is used for the host name and prompt. This means the length of the host name may cause lengthier configuration mode prompts to be truncated. For example, the full prompt for IPv6 Access Control List configuration mode is (config-ipv6-acl)#; however, if you are using the host-name Four-Leaf-Clover, you only see Four-Leaf-Clover(config-

ipv6)#. A general rule to follow is limit hostnames to nine characters or fewer.

Cisco Configuration

Cisco IOS configuration consists of statements. Each statement activates or deactivates a feature for a protocol, an interface, or the router as a whole. In addition, statements can define a global characteristic of the router, such as making all IP packets that are to be routed to a specified host, not located on either local Ethernet or token ring networks, be sent to the router at 129.1.128.1. It will then be routed to the final destination.

IOS uses exclamation points to separate sections of a configuration. Much like the pound sign in programming, you can use exclamation points to indicate comments in stored configurations; however, they are stripped out when the router loads the configuration.

To see the running configuration, enter show running-config. Our output, which is Table XII and is located in the Resources tab, is from a Cisco 7600 series router. Just as before, we recommend you open it up as a reference. Now, let's look at a few key parts of the output.

XII Table Highlights

Our example router supports the network services: timestamps, debug, datetime, localtime, and log. Their presence in the configuration file is enough to enable them. There is also a global configuration variable, hostname, which displays the router's hostname. Configuration sections that the router thinks are sufficiently different are separated by a blank line prepended with an exclamation point (!).

XII Table Highlights

This snippet from the router tells us several important things:

- The subnet-zero feature is enabled,
- The IP domain name is set to rad-turtle.com,
- The IP multicast-routing is enabled,
- The Distance Vector Multicast Routing Protocol (DVMRP) routes advertised is limited to 20,000, and
- The Cisco Express Forwarding (CEF) is enabled.

A no setting disables a service. For example, no ip finger turns the finger service off.

Cisco Router BGP

Organizations often use Cisco routers to connect multiple Internet Circuits from multiple service providers. This gives a network redundancy and high availability for access to Internet sites. It also gives external users on the Internet the best possible access to the organization. This is done through BGP, which we discussed earlier in this module.

If an organization only has one single route to the Internet for information to flow, then their network makes no routing decisions and cannot be considered an AS. As a routing protocol, BGP

announces to the whole world which IP addresses the router is responsible for and then listens to other routes to learn the best way to access other sites.

AS's via BGP

AS's exchange routing information via BGP. Two AS's that connect directly to each other and exchange routing information are considered peers. Each AS informs its peers what IP addresses can be reached in its AS, through route announcements that run using a small amount of memory. The peers reciprocate the route announcements, informing the initiating AS of the routes that can be reached through their networks. The peers also tell the AS what networks the packets will pass through to reach the destinations.

Every AS is assigned a unique number, known as an ASN, which identifies it to all devices on the Internet. The chain of ASNs that is used to get to the destination is called the AS path. The router decides where it sends the packets based on the AS path.

How Much Routing Information?

When configuring BGP, you have to make a decision. How much routing information should be received from each peer? There are three options:

- Full routes,
- Partial routes, and
- No routes.

Full routes mean that the peer will send you everything it knows about every network on the Internet. Partial routes mean that the peer only sends you routes for networks directly attached to their network. No routes mean that your router does not receive any routing information from the peer.

One of the primary reasons for wanting to receive less information from routers is memory conservation. You may decide to accept full routes from a smaller peer and partial routes from a larger peer; or, you may want to accept partial routes from a smaller peer and no routes from a larger peer, and then choose the larger peer as your default route, assuming that the larger peer has more directly connected networks than the smaller peer.

IP Blocks

Routes are designed to encompass as many IP addresses as possible in a single route statement. Whenever possible, large ISPs announce blocks /16 or larger. The smallest route announcement that is accepted by the global Internet is /24. To use BGP, and in turn be an AS, the network must have at least a /24 address block. This does not include several smaller chunks that add up to /24.

To run BGP, you must have:

- A router with at least 512 megabytes of RAM,
- Two ISPs that are both willing to provide you with a BGP feed,
- An IOS version that supports BGP version four,
- A block of /24 IP addresses,

- An ASN, and
- A routing registry entry for the network block.

ASNs have historically been two bytes; however, ARIN has recently allowed organizations to prepare for the future by offering four-byte ASNs. Nowadays, most new ASNs are four-byte numbers.

Exercise Introduction

It is time for an Exercise. In order to successfully complete the Exercise, you are expected to use your notes and any available resources presented throughout the course, in addition to conducting your own Internet research.

Routers, Firewalls, and the Internet: Section 4 Transcript

Firewalls

The main function of a firewall is to filter or block inbound and/or outbound traffic according to a configured set of rules. This has not changed since their inception; however, the complexity, coverage, and depth of inspection have improved considerably. The first firewalls in the early 1990s were IP routers with filtering rules. The early security policies were used to allow anyone within the network to access outside resources. They were also used to prevent anyone, or anything, outside the firewall, from gaining access to resources within the firewall.

These firewalls were effective, but limited, considering the difficult task of creating effective filtering rules. It was nearly impossible to identify all of the parts of an application that needed to be restricted. In other cases, people would move around, so the rules have to change.

For example, Inspector Possum's recent success, their baby-friendly fertilizer, has caused the company to go from buying anhydrous ammonia from a local supplier, to purchasing bulk shipments from an overseas distributer. This means that Lisa, the Senior Quality Control Manager of Inspector Possum, had to move from the company headquarters in Walla Walla, Washington to the distributor's location in Kuala Lumpur, Malaysia. The firewall that covers the office in Walla Walla is like an umbrella. It only fits over certain areas. So, now the rules have to be changed to cover Lisa in Kuala Lumpur.

Firewall Requirements

Early firewall requirements were easy to support, because they were limited to available Internet services. They needed to allow secure access to:

- Remote terminal services using Telnet,
- File transfers using the File Transfer Protocol,
- Electronic mail using the Simple Mail Transfer Protocol, and
- USENET News using the Network News Transfer Protocol.

Nowadays, we exponentially add to this list of requirements, due to the immense number of services available, world-wide usage, increasing number of devices and users, and the numerous ways to connect to networks such as:

- Laptops,
- Desktops,
- Mobile phones,
- Gaming consoles,
- E-readers,
- Televisions
- Webcams,

- Tablets, and
- All sorts of other smart devices.

Firewalls Today

Today, firewall functionality is built into a wide array of hardware devices, as well as almost all operating systems. No matter what the base technology is, a firewall still basically acts as a controlled gateway, filtering two or more networks through which all traffic must pass.

The National Institute of Standards and Technology Special Publication 800-41 divides firewalls into three basic types:

- Packet filter,
- Stateful inspection, and
- Application proxy.

There is a fourth accepted type, which is a hybrid, due to a mix of abilities that places them in more than one of the three defined categories.

Click the different firewalls to learn about each one.

Packet filter - Packet filtering firewalls screen packets based on addresses and packet options, by matching criteria.

Stateful inspection - Stateful inspection firewalls examine packets within the context of a new or existing session. They maintain a firewall state table to make changes to the filtering rules, based on triggering events. Someone could generate a TCP packet with a header indicating it is part of an established connection, in hopes it will pass through a firewall. If the firewall uses stateful inspections, first it verifies that the packet is part of an established connection, listed in the state table.

Application proxy - Application proxy firewalls examine the content of the communication and proxies the connection to the intended destination, so that all traffic passes through the proxy. They are also used as network address translators, since traffic goes in one side and out the other, after having passed through an application that effectively disguises the origin of the initiating connection.

Unified Threat Management

Firewalls have evolved, much like mobile telephones, and multiple functions are now built into one device. One hybrid example is the Cisco Adaptive Security Appliance (ASA), which is under the umbrella of network security products called Unified Threat Management (UTM).

In general, UTM promises integration, convenience, and protection from cyber threats. These are mainly utilized for enterprises, and incorporate firewall appliances that:

- Guard against intrusions,
- Perform content filtering,
- Filter spam,
- Conduct application control,

- Filter web content,
- Conduct intrusion detection, and
- Assume antivirus duties.

In other words, a UTM device combines functions that have traditionally been handled by multiple systems. These devices are designed to combat all levels of malicious cyber activity on the computer network. An effective UTM solution delivers a network security platform, comprised of robust and fully integrated security and networking functions along with other features, such as security management and policy management by a group or user. It is designed to protect against next generation application layer threats and offers centralized management through a single console, all without impairing the performance of the network.

ASA with Cloud Web Security

As a UTM, the ASA's Cloud Web Security and their Security Intelligence Operations integrate firewall, antivirus, intrusion prevention, and virtual private network (VPN) capabilities that deliver capabilities in many form factors for standalone appliances, blades, and virtual appliances to secure public and private network clouds. These devices use real-time, offloaded cloud-based content scanning that identifies and blocks malware and inappropriate content before it reaches the network. It also facilitates the old firewall administration issues, where people would move around and the rules would have to be changed, with acceptable use policies that can be applied to all users, regardless of location.

Let's explore two scenarios where ASA integrated with Cloud Web Security is used:

In our first scenario, Janice P. McArther, user name jpmcarther, VP of Sales at RAD Turtle Company, attempts to download their up-to-date Product_List-2015.pdf from their remotely hosted website at rad-turtle.com. As with all Internet traffic, it is redirected to the Cloud Web Security service, where it is scanned for malware and the user-based policy is enforced. Outbound traffic is classified based on user name, user group, source, or destination. The destination aspect can be further classified into three categories.

- Approved traffic is traffic from known, safe websites that is automatically approved by corporate policy,
- VPN traffic is traffic flowing through a site-to-site VPN tunnel, and
- Traffic redirected to Cisco Cloud Web Security, which is traffic sent to Cisco Cloud Web Security for granular web policy control, including URL filtering, antivirus scanning, web content scanning, and web application visibility and control.

The outbound request is from an approved user name, jpmcarther, in the approved user group CXO, going to a previously defined safe website automatically OK'ed by corporate policy. She is then redirected to the Cloud Web Security service, where it is scanned for malware and the user-based policy is enforced. Finally, Janice is allowed to download the Product_List-2015.pdf.

In our second scenario, Janice P. McArther, user name jpmcarther, attempts to download their up-to-date Product_List-2015.pdf from their remotely hosted website at rad-turtle.com, but mistypes the URL as bad-turtle.com. The traffic is redirected to the Cloud Web Security service, where it is scanned for malware and the user-based policy is enforced. Since the outbound request is from an

approved user name, jpmcarther, in the approved user group CXO, it flows until the destination aspect is reviewed. Bad-turtle.com is known for cross-site script hosting for exploiting visitors thinking they are visiting rad-turtle.com. Therefore, it is caught by URL filtering and is blocked. Janice notices the site misspelling and retries with rad-turtle.com and succeeds in downloading Product_List-2015.pdf.

Traffic Management

Firewalls may also manage traffic between two or more different networks. In the example scenario, traffic is inspected on an interface serving one network, and then it is transformed or modified if the device determines that the packet is allowed to be passed onto an interface serving another network.

Here's how network bridging works. Say you have several smart machines that have IP addresses in your home: an alarm system, a dish washer, a pet-cam, and a television. The IP addresses on these machines are then turned into the routable public IP address, which is assigned by your Internet service provider. Firewalls help keep internal traffic internal and safe from malicious external traffic. These multiple devices are behind your network device and appear to share the same public IP address, even though they are distinct systems on your internal network.

Network Address Translation

Network Address Translation (NAT) was originally developed as a temporary solution to help out with the dwindling number of IPv4 addresses. This allows globally-registered IP addresses to be reused or shared by several hosts. Traditionally, Request for Comments (RFC): 1631 has defined NAT as the maps of IP addresses from one jurisdiction to another. Although it can be used to translate between any two address jurisdictions, NAT is most often used to map IPs from the non-routable private address spaces, as defined by RFC 1918.

These addresses were allocated for use by private networks, which either do not require external access, or require limited access to outside services. Enterprises can freely use these addresses to avoid obtaining registered public addresses; however, because private addresses can be used by many, individually within their own jurisdiction, they are non-routable over a common infrastructure. When communication between a privately-addressed host and a public network, like the Internet, is needed, address translation is required. That is where NAT comes to the rescue.

NAT Routers

NAT routers, or NATificators, stand between private and public networks. Usually, they convert private addresses in each IP packet to legally registered public addresses. The NAT routers also provide transparent packet forwarding between addressing realms. The packet sender and receiver should remain unaware that NAT is taking place. Today, NAT is commonly supported by wide area network (WAN) access routers and firewalls. Let's look at two types of NAT, static, and dynamic.

Static NAT, also known as inbound mapping, is the process of mapping an unregistered IP address to a registered IP address on a one-on-one basis. Unlike static NAT, dynamic NAT does not map internal IP addresses to public addresses on a one-on-one permanent basis. Instead, dynamic NAT

maps private addresses to public addresses from a NAT pool. Because of the flexibility of dynamic NAT, they are more common than static NAT.

Edge devices provide an entry point into a network and run dynamic NAT to create connections on the fly, building NAT tables.

Static NATs create a stateless implementation of creating bindings between addresses.

Network Address Port Translation

A variation of dynamic NAT, known as Network Address Port Translation (NAPT), allows multiple hosts to share a single IP address by multiplexing streams differentiated by TCP/UDP port number. An example of how this works would be if private hosts 192.168.0.2 and 192.168.0.3 send packets from source port 1108. A NAPT router translates these to a single public IP address, 206.245.160.1, and two different source ports, 61001 and 61002. Response traffic for port 61001 is routed back to 192.168.0.2:1108, while port 61002 traffic is routed back to 192.168.0.3:1108.

NAPT Masquerading

NAPT masquerading is commonly implemented on small office and home office routers. Masquerading allows an entire LAN to use a single public address. Because NAPT maps individual ports, it is not possible to reverse map incoming connections for other ports unless another table is configured. A virtual server table can make a server on a privately addressed demilitarized zone (DMZ) reachable from the Internet, via the public address of the NAPT router. This is a limited form of static NAT applied to incoming requests.

In some cases, static NAT, dynamic NAT, NAPT, and even bidirectional NAT or NAPT may be used together.

Exercise Introduction

It is time for an Exercise. In order to successfully complete the Exercise, you are expected to use your notes and any available resources presented throughout the course, in addition to conducting your own Internet research.

Routers, Firewalls, and the Internet: Section 5 Transcript

Summary

You have completed the Routers, Firewalls, and the Internet module.

Within this module we discussed the roles of core network components as the gates of network traffic, and their inherent handles and locks used for filtering packets to the desired route and destination.

You should now be able to:

- Describe Internet Protocol (IP) network filtering devices,
- Describe Autonomous Systems (AS),
- Identify how Regional Internet Registries (RIR) relate to AS Numbers,
- Explain IP network address translation (NAT),
- Explain IP network address port translation (NAPT),
- Recognize the differences between various firewall types, and
- Translate router configurations for network communication.

To receive credit and advance to the next module, you must achieve a passing score on the Module Exam. Click the Next Section button to begin the Module Exam.