



Romel Cabling ▾



Home

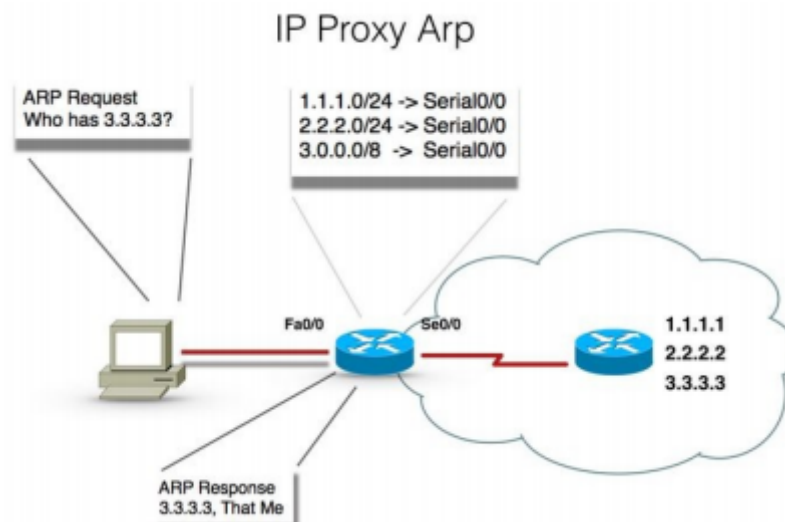
Home > My courses > 121 - ITSP2B > 16 Exploring Firewall Technologies II > Lesson Proper for Week 16

Lesson Proper for Week 16

TRANSPARENT FIREWALL

As an additional security measure, we have the transparent firewall. In a traditional configuration of networks, a firewall acts as a router or default gateway for the hosts that connect to its filtered subnet. We have a Layer 2 firewall, known as a **transparent firewall**, which acts like a covertness firewall. These types of firewalls are used only when a gateway of web proxy or antispam is needed, and they should have features such as Proxy ARP and disabling NAT.

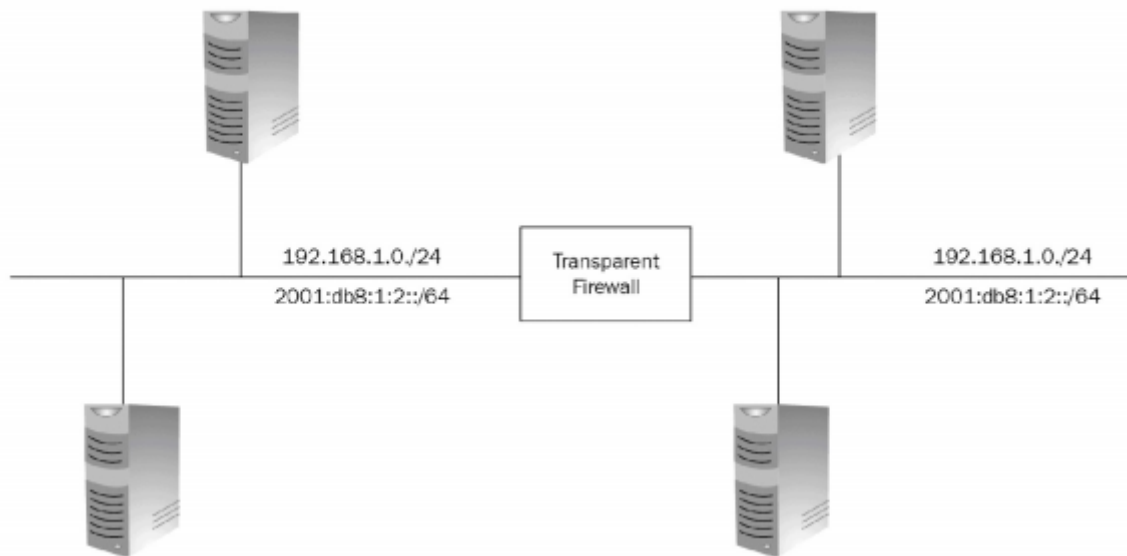
Proxy ARP is a technique where a device answers an ARP request intended for another device:



The characteristics of a transparent firewall:

- The transparent firewall mode supports inside and outside interfaces
- It can be run on a single as well as multiple context modes
- Packets are bridged by the security appliance from one VLAN to the other, instead of being routed

- MAC lookups are performed rather than routing table lookups



A transparent firewall can be introduced very easily into an existing network, since it's not a routed hop and it doesn't require an IP address. There are no routing patterns or NAT configurations, and very little troubleshooting. The transparent mode acts as a bridge but still, it doesn't allow Layer 3 traffic to pass through security appliance from a lower security level interface to a higher security level interface.

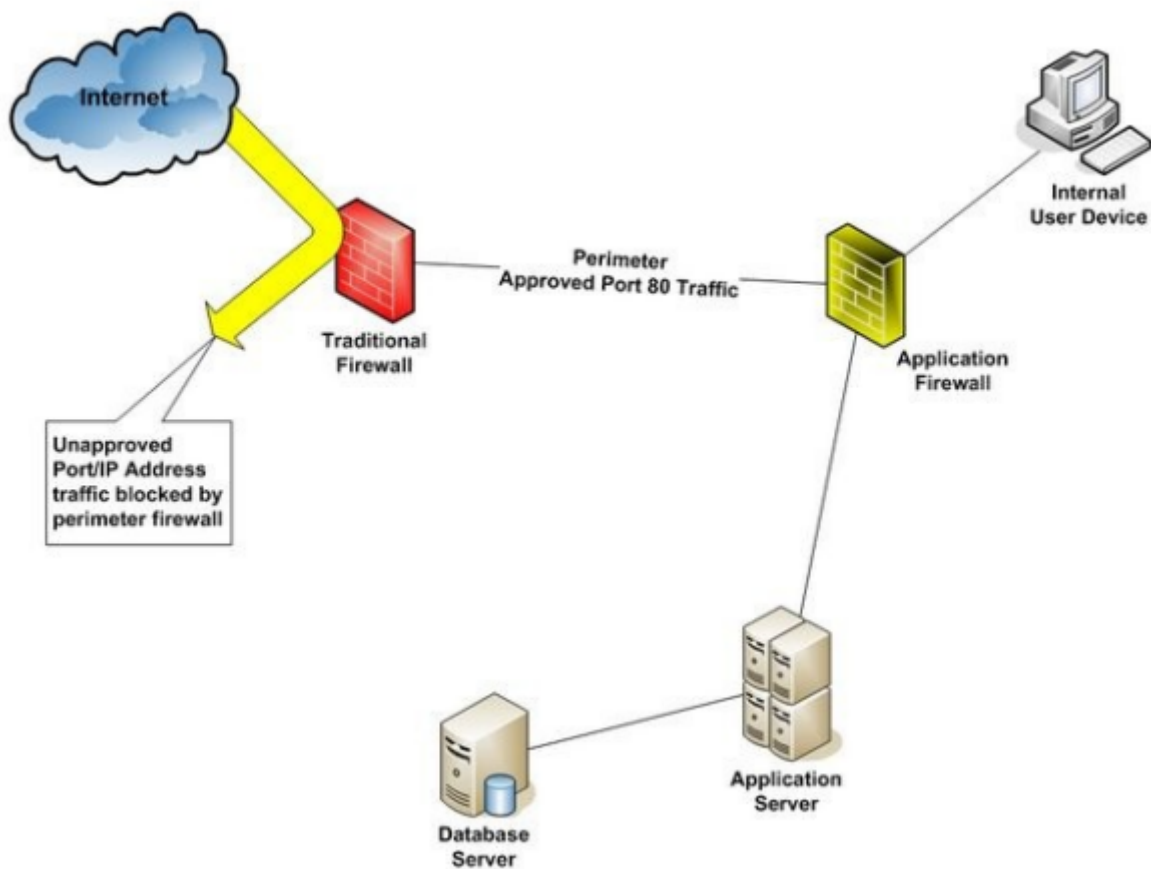
We can control the passage of traffic with ACL, either extended or EtherType ACL. If no ACL is configured, then it would only allow ARP traffic, which can be controlled by ARP inspection. It also doesn't allow CDP packets or any other invalid EtherType packets greater than or equal to 0x600. For example, the IS-IS packet is not allowed but will allow BPDUs.

One should consider the fact that as an L2 device, the security appliance must be on a different VLAN to keep it secured from any accidental access.

APPLICATION LAYER FIREWALLS

The application-layer firewalls are also known as **proxy firewalls** or **application gateways**. They allow the greatest level of control and work across all seven layers of OSI. The filtering effect takes place at layers 3, 4, 5, and 7.

Many application-layer firewalls include some specialized application software and proxy servers. Specific traffic, such as FTP or HTTP, is managed by the proxy server. These servers are specific to their original design for the protocols. They help in report generation for auditing purposes by providing enhanced access control and validating every piece of data:



Proxy firewalls serve as an intermediary between networks, such as the internet and the company's internal network. In a proxy firewall environment, there isn't any direct connection. The proxy servers provide the only visible IP address on the internet. The client connects to the proxy server to submit their request pertaining to Layer 7, which includes destination as well as data. Based on the configuration on the proxy server, it can analyze, filter, or change the data itself before processing. It can make a copy of all the incoming packets and change the source address, in order to hide the internal address from the outside internet world, before it is sent out to the destination. And when it receives a response from the destination, it becomes its responsibility to ensure the delivery of that response to the right client.

The following are some benefits of application-layer firewalls.

1. Authenticates individuals and not devices

This implies connection requests are authenticated before traffic is allowed to cross an internal or external resource. This ensures authenticating the user/individual instead of a device trying to connect.

2. It's more difficult to spoof and implement DoS attacks

Application-layer firewalls help in preventing most of the spoof attacks, and DoS attacks are limited to the firewall itself. This helps in reducing the burden on internal resources.

3. Can monitor and filter application data

Application-layer firewalls allow an administrator to control what commands and functionality rights/access are given based on their role, the required authentication, and the information pertaining to it.

4. Logging information in more detail

Logs are generated with such detail that you can monitor the actual data an individual is trafficking it across. This also helps in tracking various new ways of attacks, since we can monitor how a hacker is trying to crack into the system. Logging would also prove more useful to trace the amount of bandwidth being used by an individual resource, the sites that are being accessed, and which resource is being utilized most often.

5. Working with the application-layer firewall

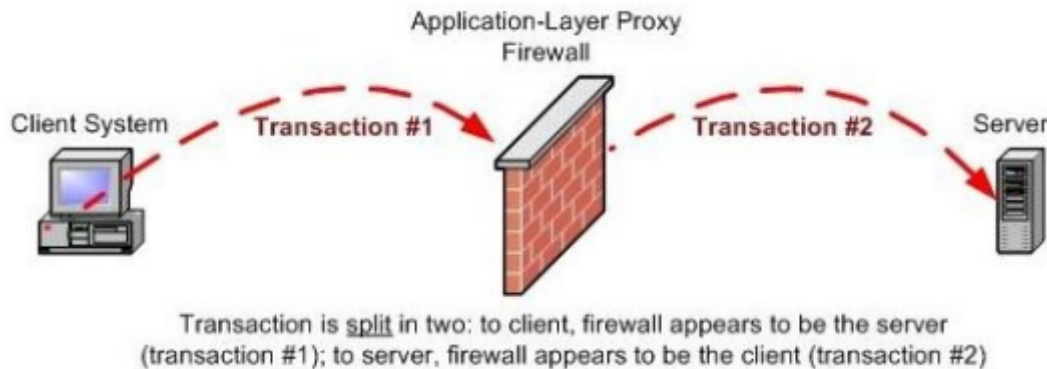
Application-level proxy firewalls control how internal users are accessing the outside internet. They do it by running a protocol stack for each type of service that they want to provide. In some network environments, we can see that the proxy servers are used to block all incoming traffics and allow only the internal resource to access the internet.

6. Application-level proxy server

The proxy server is a computer or a router that interrupts the communication between customer and provider and acts as a relay. They generally prevent the attacker from entering into a private network.

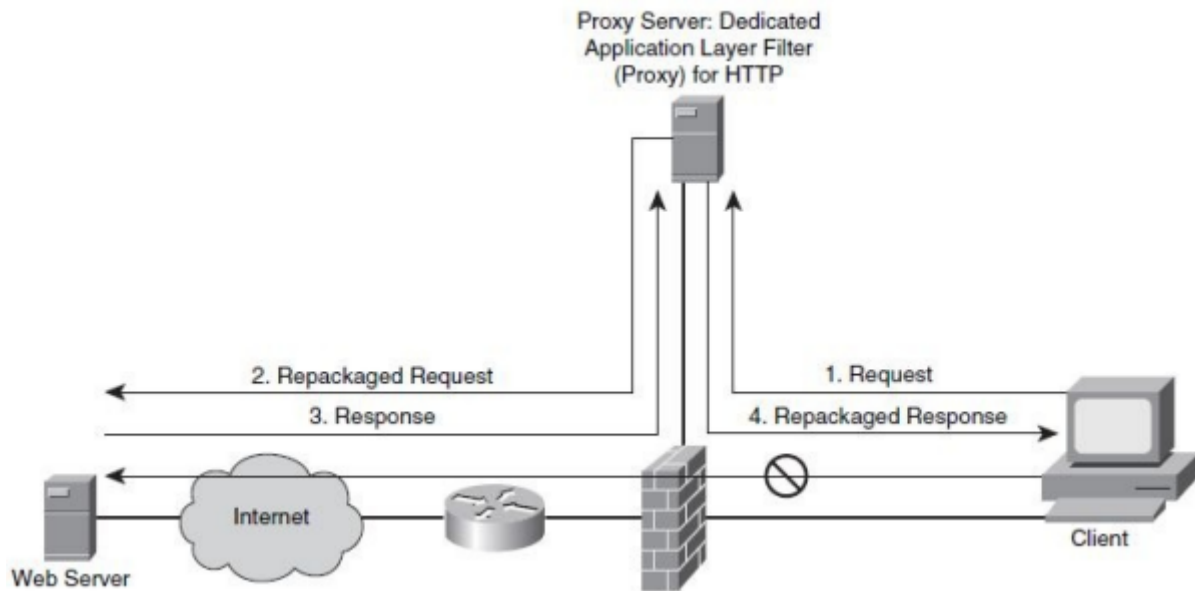
The application-level proxy server is a form of proxy server that is specific to a particular application and protocol. They have complete information about the content of the packets.

SOCKS is an IP-based circuit-level proxy server software that supports TCP and UDP applications:



7. Typical proxy server deployment

The following figure shows how a proxy server can be deployed in an environment. One interface of the router is connected to the internet and the other to the client. When the client requests a connection to the internet, the proxy server receives the requests, checks the request, and repacks the request. As an application-level firewall has information about the packet, they are processor sensitive. These firewalls are also protocol-specific so they use more memory to process a request:



Let's understand how the process works:

1. The proxy server receives a request from the sender/clients
2. The server performs user authentication according to the norms/configurations made into it
3. It forwards Layer 3 and Layer 4 packets to check the rules of the firewall and tries to access the requested website using the internet
4. The proxy server returns the request of the client; the proxy server forwards only Layer 5 and Layer 7 messages and the information allowed by the server

The main reason behind the architecture of application-layer firewalls is solely to provide the highest level of filtering for a specific protocol. Despite everything, the proxy server lowers the speed of network performance since it needs to evaluate the most significant amount of information embedded in packets.

Areas of opportunity

Application-layer firewalls are very processor-intensive; they require a lot of memory and CPU cycles to process every packet that needs to undergo scrutiny. The detailed logging is quite beneficial, but still, that consumes a lot of resources within the device. Two solutions have been designed:

- Using COTP (short for, Context Transfer Protocol) to authenticate and authorize, instead of monitoring the data on a connection
- Ensuring that layer firewalls would monitor the imperative applications, as per the company requirement only

Additionally, there are some other limitations, such as they don't support all applications, since the monitoring has a limited number of connection types— Telnet, FTP, or web services. Another limitation is that they require vendorspecific software, which limits the scalability and may create management issues.

8. Packet filtering and the OSI model

Static packet-filtering firewalls act as L3 devices. Filtering and ACL rules are applied to determine the acceptance/rejection of a packet from a particular source, destination, IP address, port number, or packet type. The strategy is to check whether any packet is trying to enter the internal network from the external claiming to be an internal packet.

As we are already aware, each service has a port number assigned to it. So packet-filtering can be done based on port numbers. A simple way is to block the port number to block a particular service. For example, if a Telnet service needs to be blocked, then you can simply block port number 23 and restrict the access of the Telnet service.

Static packet-filtering firewalls are similar to packet-filtering routers, but there is a slight difference. The filtering firewalls are very scalable and application-independent in nature, hence they have high performance standards

◀ Preliminary Activity for Week 16

Jump to...



Analysis, Application, and Exploration for Week 16 ▶



Navigation

Home



Dashboard

Site pages

My courses

121 - CC106

121 - BPM101 / DM103

121 - OAELEC2

121 - ITE3

121 - MUL101

121 - ITSP2B

Participants



Grades

General

01 Exploring Security Threats

02 Delving into Security Toolkits

03 Intrusion Prevention System

04 Understanding Security Policies I

05 Understanding Security Policies II

06 - Preliminary Examination

07 Deep Diving into Cryptography

08 Deep Diving into Cryptography: Types of Cipher

09 Implementing the AAA Framework


10 Implementing the AAA Framework: Implementing A...

11 Securing the Control and Management Planes


- 12 - Midterm Examination
- 13 Protecting Layer 2 Protocols
- 14 Protecting the Switch Infrastructure
- 15 Exploring Firewall Technologies I
- 16 Exploring Firewall Technologies II


 Preliminary Activity for Week 16

 **Lesson Proper for Week 16**

 Analysis, Application, and Exploration for Week 16

 Generalization for Week 16

 Evaluation for Week 16

 Assignment for Week 16

17 Cisco ASA

121 - WEB101 / CCS3218

Courses

Fair Warning

NOTICE: Please be reminded that it has come to the attention of the Publishing Team of eLearning Commons that learning materials published and intended for ***free use only by students and faculty members within the eLearning Commons network were UNLAWFULLY uploaded in other sites without due and proper permission.***

PROSECUTION: Under Philippine law (Republic Act No. 8293), copyright infringement is punishable by the following: Imprisonment of between 1 to 3 years and a fine of between 50,000 to 150,000 pesos for the first offense. Imprisonment of 3 years and 1 day to six years plus a fine of between 150,000 to 500,000 pesos for the second offense.

COURSE OF ACTION: Whoever has maliciously uploaded these concerned materials are hereby given an ultimatum to take it down within 24-hours. Beyond the 24-hour grace period, our Legal Department shall initiate the proceedings in coordination with the National Bureau of Investigation for IP Address tracking, account owner identification, and filing of cases for prosecution.

2nd Semester Enrollment

A banner for Bestlink College of the Philippines (BCP) featuring a blue-tinted image of a modern building. The text is overlaid on the image. At the top right, it says "visit www.bcp.edu.ph". The main headline in large red letters reads "Enrollment registration is now Ongoing". Below this, in white text on a blue background, it says "For 2nd Semester SY 2021 - 2022". Underneath that, in white text on a blue background, it says "We are accepting new students, returnees and transferees." On the right side, there is a quote: "Be trained to be the best, Be linked to success" next to the BCP logo. At the bottom left, there is an email icon and the address "bcp-inquire@bcp.edu.ph". At the bottom right, there is a phone icon and the numbers "(8)442-8601 | (8)518-8050".

visit www.bcp.edu.ph

Enrollment registration is now Ongoing

For 2nd Semester SY 2021 - 2022

We are accepting new students, returnees and transferees.





"Be trained to be the best,
Be linked to success"



 bcp-inquire@bcp.edu.ph

 (8)442-8601 | (8)518-8050

Activities

-  Assignments
-  Forums
-  Quizzes
-  Resources

Bestlink College of the Philippines
College Department

Powered by [eLearning Commons](#)