

12.2.2 Reconfigure and Protect Endpoints Facts

This lesson covers the following topics:

- Application endpoint protection
- Endpoint security configuration

Application Endpoint Protection

Applications are allowed to enter a network via a firewall. In order to keep malicious apps from entering, you must create rules that allow or deny specific applications. This process is referred to as whitelisting and blacklisting. You can also quarantine an application. The following table describes these processes.

Process	Description
Whitelisting	<p>Whitelisting allows an IT admin to control the applications, IP addresses, URLs, and email addresses that are allowed onto the network. Whitelisting can be done at the firewall, email server, or using applications that automate updates and virus protections. Whitelisting is a great tool, but it is much more labor intensive than blacklisting.</p> <p>Whitelisting might mistakenly fail to list a needed application and interrupt work-flow.</p> <p>Remember, whitelisting denies access until the item is added to the whitelist. This is called implicit deny. This is part of access control and is more strict than blacklisting.</p>
Blacklisting	<p>Blacklisting is the opposite of whitelisting. An IT admin can list the applications, IP addresses, URLs, email addresses, etc., that are to be blocked from the network. This can also be done at the firewall, email server and application.</p> <p>Blacklisting is considered easier to do since the lists tend to be smaller. It is also possible to subscribe to blacklists produced by security companies. These lists are updated regularly, sometimes daily. These subscription blacklists are compiled from information provided by thousands of companies that report malicious applications, IP addresses, and email addresses. This makes using blacklisting easy and automated. The best practice for utilizing blacklisting is to integrate a next-gen security platform that offers a cloud-based master database of threats.</p>
Quarantining	<p>When anti-virus software finds a malicious item it quarantines it. This means that the item is placed in a folder where it cannot cause any damage to the network. If it is found to be non-malicious it can be released from quarantine.</p> <p>Endpoints are the devices that attach to a network, such as desktop computers, laptops, smartphones, printers, etc. Endpoints represent a prominent attack vector. These endpoints, when attacked, become pivot points to deeper network assets. An endpoint can be quarantined. If this is done, the endpoint will no longer receive network traffic.</p>

Endpoint Security Configuration

Endpoint security requires constant maintenance. This may mean changing an endpoint security configuration to improve the security posture. The following table describes tools you can use to enhance endpoint security.

Tool	Description
Firewall rules	Define how a firewall is configured. The natural state of a firewall is implicit deny, meaning

	that communication must be allowed by a network admin. Firewall rules specify the data that can enter or leave the internal network. These rules are the frontline security for the network and must be carefully configured.
Mobile device management (MDM)	Mobile devices now outnumber traditional network devices. These endpoints present unique challenges since the devices are not physically protected by locked office doors. MDM offers a way to easily monitor and manage mobile devices including updates, data encryption, and remote wipe of a compromised device.
Data monitoring apps	A concern of organizations is data being downloaded. A variety of applications help an admin monitor data. These apps monitor data in all three states: at rest, in motion, and in use.
Content filters	Content filtering is a strategy to keep employees from accessing unauthorized content on the web. Online URL filtering is based on selected objectionable content. This tactic is also used with emails that help to combat phishing. Filtering is often deployed at the firewall but can also be deployed using other tools.
URL filters	URL filters are a database of URLs that are allowed (whitelisted) or prohibited (blacklisted). While the database can be created and maintained manually, most are regularly updated databases that are SaaS in nature. Machine learning is used to improve the accuracy and the speed of updating these database.
Certificate status databases	Trust is an imperative when accessing websites. Certificates provide this trust. Certificate databases provide easy access to certificate status (valid, invalid or revoked). Certificates can be revoked for any number of reasons by the CA. Many browsers block websites with invalid certificates.

Copyright © 2022 TestOut Corporation All rights reserved.