Sophos UTM – SSL Web Proxy Scanning Configuration and GPO Deployment

Posted on March 19, 2017 | by Travis G | Posted in HowTo

This document will provide instructions on how to implement SSL Scanning to filter websites that use HTTPS on a Sophos UTM firewall.

Home editions of Sophos UTM are available Free here, however please note that you do have to register with Sophos to receive your free license. You can run this as a physical server using a small PC or a Virtual Server on ESXi/HyperV.

Requirements:
– Access to manage the Sophos UTM
– A test computer on the network subnet that SSL Scanning is being enabled for.
– Access to the Active Directory Server and GPO management.

1. Log into the clients Sophos Router
   https://SophosIPAddr:4444
   1. Use your credentials to log in

2. Go to Web Protection, Web Filtering, HTTPS CAs and click on Download under Signing CA
   DO NOT CLICK REGENERATE. If you do then the existing certificate deployment will fail and you will have to do this all over again.

3. Use export type PEM. Click Download**.**
4. Now that we have the SSL certificate that is needed to enable HTTPS scanning we will need to import it into group policy. Open Group policy and edit the default domain policy if you want it to apply to the entire domain. Or you can create a new GPO and link it to whatever OU you want it to apply to.

5. Go to Computer Configuration, Policies, Windows Settings, Security Settings, Public Key Policies, Trusted Root Certification Authorities

6. Here you can see I already have a Proxy CA certificate. Yours might be called something else but it will have the word proxy in it. Since I need to reimport it, so I will go ahead and update this. If you need to update it, first **Delete the existing Proxy CA**. Then right click and select import.

7. Click Next and browse for the certificate you just downloaded. When you browse you may have to select All Files to see the certificate. Use the date modified to your advantage because sometimes you might have multiple certificates show up.

8. Make sure Trusted Root Certification Authorities is selected and click next.

9. Click Finish

10. Now we have the Proxy CA

11. Verify all the Domain Controllers replicate this.
12. Now we need to check and make sure they do not have block inheritance on any OUs with computers. Typically people don’t use this but you need to double check and

Scanning – Step 9 CA Cert Deployed with GPO

Recent Comments

Archives

- March 2017
- February 2017

Categories

- HowTo

Meta

- Log in
- Entries RSS
- Comments RSS
- WordPress.org

make sure. Here you can see the blue exclamation marks which means they have block inheritance on. That means these OUs will not get the default domain policy. **DO NOT CHANGE ANY OU settings**. **Do not use Enforced settings.** Just make the changes explained in this document that need to be made to get the certificate installed. Do not make any changes that can impact users.

13. So in this example, Netbooks, Student, Tablets, Windows 8, need to have the newly created group policy linked. Fo each OU and Link the new Install Proxy Certificate. Remember this certificate is install on the computer level not user level. So the Students OU wouldn't matter since it just contains student accounts.

14. Now that we have the certificate deployed to Active Directory we need to have all computers restarted. When they restart they will install the certificate. Restart your test computer. Alternatively you can run gpupdate /force from command line.
15. Now we need to enable SSL scanning. In the Sophos UTM, go to Web Protection, Web Filtering Profiles, Filter Profiles.

16. Edit All of the profiles and select HTTPs and select Decrypt and Scan and click Save.

17. Make sure you enabled Scan HTTPS for all of the profiles. Now on the test computer open up internet explorer and go to https://www.bankofamerica.com. If you get a certificate not trusted warning then you need to restart.
18. If you are using a Standard Proxy instead of Transparent, you need to make sure you have a "FallBack" filter profile. This profile is used to ensure that anyone without proxy settings at least gets filtered transparently. So under Webfiltering Proxy Profiles in this screen shot you can see that there is a proxy fallback profile.

    If you don't have one then follow these steps

    1. Click New Proxy Profile

2. The name should be called fallback. The position should be bottom. We want this to be very last. The network should be the LAN internal Network

3. Make sure Fallback action is set to the most restrictive Filter. This is important! Then make sure operation mode is transparent. Authentication type is none. Full transparent is UN-CHECKED. Make sure Decrypt and Scan is checked in HTTPs tab.

4. Click Save.
5. So now if you go to a device that does not have proxy settings in internet explorer and view the Sophos Live Log you should see that device profile listed as fallback.

19. Now if you need to install the certificate on the IPADs then go to http://passthrough.fw-notify.net/cacert.pem. When the IPAD tries to access that site behind the Sophos it will pop up with an option to install the certificate. Note an IPAD may require the PKCS cert exported from step 2.
20. The client should do some extensive testing to ensure the sites the need to access work.

‹ OPNsense – Transparent Caching Filtering Proxy with Virus Scanning – Step 10 Final Steps

FreePBX – Setup SIP Trunk Through Callcentric ›

Tagged with: firewall, proxy, sophos