NetSpective Evaluation Calls

1. An introductory email is sent by the Sales person and a time and date is scheduled for the Evaluation Call. The Sales Engineer sets up the WebEx Invitation and supplies the Dial in number for the related conference bridge, which is then forwarded to the Customer.
2. Intro - On the day and time, meet in the designated conference room. Start up your WebEx session and dial in to the appropriate conference bridge.
   - **2.1.** When the customer comes into the call, after the introductions you should set their WebEx as the host so they may share their screen. This will allow you to direct them as they configure their evaluation appliance.
   - **2.2.** You may want to get some feedback from the customer at this point. Will the customer want to integrate LDAP groups and users for the entire organization or just for a single user to start with? They may just be interested in leaving the appliance in log mode and familiarizing themselves with its features, or just look at reporting.
3. Manually Give NS an IP Address - Some of the more basic things may or may not have been applied yet. You should note that the Appliance needs to be set up inside their network for features such as LDAP Authentication to work and communicate properly.
   - **3.1.** Ask if the customer has given the NetSpective Appliance an IP address yet. If they haven't, they will need to plug a monitor and keyboard into the appliance. The default login credentials are "Admin" and "webfilter" without quotations. The first option "1" will direct them to the area where they can configure an IP address into the device. When finished, they can hit "0" to leave the menu system. They may now access NetSpective from any computer by using their web browser and navigating to the IP address they used on the appliance.
4. NetAuditor 3 - If Net Auditor 3 is not installed, you should demonstrate how to install and set it up. The Net Auditor 3 client can be downloaded from the **Utilities** section. After downloading and installing it, when we run the program it will initially ask us if we want to automatically configure NetAuditor's settings. Click on "OK" each time and it should automatically set up a Syslog connection for them.
   - **4.1.** There may be updates for NetAuditor. Have them navigate to the Help menu of the NetAuditor application and click Install Update.
   - **4.2. Net Auditor** Ensure that the customer has properly setup NetAuditor and that it is collecting data. In our first evaluation the customer had already set up NetAuditor. Further instructions will follow when I have them.
   - **4.3. Device Settings -> Logging [Syslog Settings – TCP]** If you are having issues getting the logs to show, you may want to double check that the Syslog server is set to TCP, the IP address is pointing to the server that NetAuditor is on, and timestamp is enabled. If not, this could cause some minor loss of log data.
   - **4.4.** If the customer is curious, NetSpective's Syslog streaming is smart enough to hold the logs and resend them in the event the NetAuditor service or the link to NetAuditor goes down for any reason.
5. LDAP - Most organizations are leveraging a directory service and will want to see all their groups and users imported into NetSpective and you can't filter and report without users.

5.1. **Groups [Configure LDAP Sources] [Add] or Device Settings -> LDAP Sources [Add]–** This is where we can configure NetSpective to read group and user information from the LDAP source. Have them enter a Name, select a LDAP type from the drop down menu, Enter the NetBIOS Domain name, IP address, Login & Password info for a guest account that has read only access (Ex. TELEMATE\test.account), and Search Base terms (Ex. Dc=telemate, dc=net) without spaces.

5.2. In the event that the customer wants to use the Hostname for the LDAP source instead of the IP address, you will need to have them add DNS servers to the NetSpective appliance. Head over to the **Device Settings -> Network** area and on the left they can enter the IP addresses of their DNS servers. Make sure they click "OK" instead of hitting enter to add the IPs as there is a bug where they won't show up in the list if they just hit enter.

5.3. For Windows NTLM authentication using the portals **- Device Settings -> Advanced (Join Button)** This is where you can enter the related information to have the NetSpective appliance join the LDAP domain. Please note the "Domain" is the NetBIOS name, where the "AD Realm" is the full name. Ex. Domain = TELEMATE , AD Realm = telemate.net

6. Portals - If the customer wants to create a single user for themselves without using logon agent authentication, the best place to start is with the Portal. With this method, we can avoid having to statically assign a user or dynamically assign one with a Logon Agent. It is a simple and fast way to filter a single user.

6.1. **Filter Settings -> Authentication** is where this can be found. Have them enter their IP address with a Subnet Mask of /32.

6.2. LDAP authentication will cause them to hit a redirect page that will ask for their LDAP credentials in order to authenticate and proceed. Windows NTLM however will not redirect them to login page. The only downside is that it will only work in a Windows environment.

6.3. Back on the **Filter Settings -> Authentication** page, you should now see the user's IP address under Authentication Ranges. IP/Netmask rules are evaluated in order from top to bottom and the first matching rule is used. You will find the arrows on the right side and use them to move the new IP range to the top of the list.

6.4. If everything has been set up properly, the customer can proceed to test the Authentication Portal. Have them navigate their browser to a webpage. If you chose LDAP authentication, they will hit a page where they will be asked for their credentials. You should them have them click on the **Statistics** page in NetSpective and search for their IP address. This will confirm that they are being filtered and logged.

7. **Groups -** Exempt and Public groups are in the appliance by default and should be talked to. Anyone in the Exempt group will not be blocked. The Public group typically blocks all traffic and is intended for guests who join the network without Authentication. The Public group is typically referred to as a "Catch-all".

7.1. At this point you can walk the customer through the steps for adding a new group. The **Add** button in the upper left corner will open up the window for creating a new group. Be sure to create this group using the LDAP Source and LDAP Object features to show the customer how easy it is to add groups from their Directory.

7.2. Briefly talk to the other features on this window such as Alternate Days policy, YouTube for Schools, Block Override, Abuse Settings, and Managers. You most likely won't need to set up all of these right now, but the customer should be familiar with their use and location.

8. **Block Page Overrides -** In order to enable the Override Text on the block page, you must first enable block page overrides. From the Groups section under the Management heading, go into one of your groups such as the Public group. From there go to the Block Override tab and enable one of the Override modes, such as Group Override (with this the override will be in effect for the entire group). The duration is set to 15 minutes by default as well as the Manager Credentials option is checked under Authentication (must have a manager capable of issuing block page overrides for this method of authentication to work). Click OK to save your changes. The override text options should now show on the block page.
   8.1. To customize the Block Override Page, you can navigate to the Filter Settings -> Customization -> Block Page section of NetSpective, found under the System Control heading on the far left. From this page, you can edit any of the areas of the block page you wish. There are also toolbar icons above the editable windows to insert predefined macros for various things such as the blocked URL, the group the user is in, or the duration of the override, etc. You may add HTML code and scripts to these windows if you want, just be aware that any script code should be all on one line or they won't work.
9. **Filter Settings -> Advanced, Enable Browser Protection -** This will put the Browser Protection category in the Group Policy section. This includes the Malware and Phishing sub categories.
10. **Group Policy -** Now that we have a user as well as a group; we can begin filtering that group. First talk to the **Save To** feature. They'll want to know that it's easy to replicate any of the filtered settings to new groups that they'll make in the future. Then just explain all the other features of Group Policy, giving an overview of all the categories which have sub categories.
    10.1. Make sure to have the customer enable the Micro Updates feature, which is off by default. Navigate to the Updates menu and click on the link next to it, which typically says "Current". Explain what Micro Updates are and check Enable Automatic Update. Micro Updates should also be listed as Every 10 Minutes.
11. **Overrides -** Give a general explanation of all the features of Overrides such as Import and Export, Categories, Start and End dates, and Reference Depth. Also note to the customer that while in the Overrides section, the System group applies overrides to all other groups.
12. **Users -** If you have followed the previous steps for LDAP integration, the Users section should now be populated. This feature generally takes a small amount of time to get the user and group information from the LDAP source and populate NetSpective. That is why we wait until now to check it.
13. **Managers -** If asked, explain the features of the Managers section, particularly the Security Levels.
14. **Utilities -** Explain how the Logon agent and Remote agents work. Note that the Mac Logon Agent actually needs to be installed on the device where the Windows and Citrix ones can live on the domain server and run based on Group Policy Objects or Network Logon Scripts.
    14.1. You may also want to talk about the **Remote Agent** section. As noted in the header, you may enter the internal and external addresses for your devices as well as open the default port of 3001. If you need to verify that the Remote Agent is functioning and communicating with

NetSpective, type into your address bar: 127.0.0.1:4000/stats . This should show you the internal and external IP addresses of the NetSpective.

14.2. If you didn't create portals earlier for unauthenticated users, make sure you tell the customer about our portals. **Filter Settings -> Authentication** You can talk to the zone based portals and the methods of authentication. Make sure you also tell them about our mobile compatible portals with pairing feature that at the time of this writing is currently in QA.

15. Reporting **Statistics –** If you haven't visited the on-the-box reports for testing yet, give a brief overview of them now. Talk to the search engine.

16. **Configure Reports** - Give an overview of the reports. Talk to the frequency you can set (scheduled and custom saved reports), the formats and customization, and the various filters. Then show off the completed reports, noting things like the speed at which reports are run, how we store reports and how they are pruned.

17. **Security Manager -** Explain the ability to sync manager logins from NetSpective. This way any managers you may have created in NetSpective can be transferred over to NetAuditor.

17.1. **Manager Properties** - Now would also be a good time to go over the properties of the managers here in NetAuditor and the features shown. Discuss how managers can be set up so that they only see the reports and have the ability to report on only the groups that they want to see.

18. **Monitors -** Explain the features of the monitors. Click the Add a New Line to the Monitor and explain the filtering and alarm features.

19. Follow Up with the Customer **-** As that wraps up the Evaluation demonstration, you should email the customer your contact information and tell them they can send you any feedback and questions that they may have. Ask them for a day when you can follow up with them so they may ask any further questions they may have.