ScanSafe On ISR-G2 - FAQ's

1. What is the purpose of source interface under content-scan parameter-map?

   Source interface/IP Address is used to replace the client IP address when sending a request to the scansafe tower. In the upcoming IOS releases this CLI will be an optional one, right now it's mandatory.

2. Under dual ISP scenario, which interface needs to be used as source interface?

   In case of dual WAN scenarios, it would be better to configure a loopback interface and then make that as the source interface/ip-address under the parameter-map. So even if one link goes down and comes back, that shouldn't have any impact on the scansafe feature.

3. Scansafe Tower not coming UP?

   - ✓ Make sure the scansafe tower hostname can resolve to a proper Scansafe Tower ip address.
   - ✓ Check for proper ACL,DNS, NAT & Routing
   - ✓ Check for Scansafe License.
   - ✓ Make sure NTP is configured on the Router.
   - ✓ Make sure that there is no upstream device which can block the scansafe tower request.
   - ✓ Users can enable debug content-scan control-plane CLI to verify actually what's going on with the tower. (DNS Resolution, TCP Ping, GST Check.)

4. What is the maximum length of a single user-group supported?

   64 bytes (or Characters)

5. Are there any known limitations wrt large amount of groups?

   A single user-group can be upto 64 chars and the total user-groups length all together should be 1200, after that it will just truncate the remaining part of the user-groups and send it to the scansafe tower for policy applications.

6. Is there a limit on the HTTP header size set by default on the ISR (for upstream devices like ISA which might reject packets based on a large header size because we are adding the x-scansafe headers)

   There is no such limit on ISR.

7. What is whitelisting? (Traffic exceptions)

   We can directly forward the traffic to the actual webserver instead of scansafe tower, the traffic can be controlled using IP (through ACLs), host based (using regex), user-agent (eg: Mozilla, Chrome, Safari..) user & user-group based whitelisting.

8. Whitelisting Order?

   Say different types of whitelisting configured on the box, the order of precedence will be.

   IP Based

   User/User-group Based

   Host/User-Agent Based

9. What license is required to enable Scansafe on ISR-G2?

   Customers need to buy the security k9 bundle to enable the scansafe feature.

   Customers need to buy the per seat based scansafe license depending on the number of users (seats) who will be using the scansafe service.

10. What is the default order of preference for the user-groups?

    User-groups learned through any Authentication method.

    Default user-group under the ingress interfaces.

    Default user-group under global content-scan parameter-map.

11. What's the purpose of virtual-ip & virtual-host in the ip admission rule?

    Virtual-IP & Virtual-host is mainly required for Transparent NTLM Authentication, by defining a virtual-host, initial web requests are redirected to the virtual-host first which is part of the trusted domain and hence the box thinks that it belongs to the same trusted domain and doesn't prompt for the user authentication, for this same trusted domain (LDAP) configuration should be available on the ISR.

    The Virtual-ip & virtual-hostname should be unique in that network and the virtual-host must be DNS resolvable. Don't configure the virtual-ip address on any devices in the network, including the actual ISR-G2 itself. This also includes loopback interfaces -- do not configure the virtual-ip address on any interface on the ISR-G2. We have seen some engineers try to do this when the try to "ping" the virtual-ip address and receive no response from the G2.

    The virtual-ip is not icmp ping reachable — so the virtual-ip address will never ping. Because the virtual-ip address lives inside the ISR-G2, when the client browser is redirected to the virtual-ip (or virtual hostname) the client computer will try to make a layer-4 TCP socket connection to that virtual-ip address and that connection attempt must be routed to the ISR-G2, so that the ISR-G2 can recognize that IP and complete the three-way TCP socket connection with the client browser. If the client PC has multiple NIC cards, please configure a static route for the Virtual-IP to go through the ISR-G2.

    NOTE: Transparent NTLM Authentication works mainly in the windows world, users should have logged into the same domain as what was configured on the ISR. Transparent NTLM Authentication may not work for the smart devices such as (Android Based Phones, iPhone's, iPADs, etc)

    iOS & Safari do supports NTLM Authentication, but they don't support Transparent NTLM Authentication, having said that, If end-user/customer enters the username & password for the first time in his/her iPAD it will cache that user/password info and use that for any subsequent request and it will never prompt for the authentication unless the user manually clears the browser cache. So it means after the first authentication, the user experience will be very much

similar to NTLM Transparent Authentication. This is tested with Apple – IPAD2 - IOS 5.1.1 using Safari Browser.

To make this work, we need a minor change in the ISR-G2 config for virtual-host.

Eg : Say if the virtual-host name is isrproxy and the domain name is cisco.com, then the virtual-host needs to be appended with the domain name. [isrproxy.cisco.com]

We need this config change, because the iPAD's are not generally, any part of the domain, hence we need to explicitly append the domain name in the virtual-host to resolve the virtual-ip.

12. Authentication methods are always integrated with Scan safe?

    No.

    Authentication methods and scansafe redirections are two independent features on the ISR-G2, it's up to the customer whether they want to club it together for the user granular policy or not. Earlier authentication methods are used to control the user's policies, but with scansafe the authentication methods are used primarily for user granularity for policy application.

    If an organization has just a flat structure in terms of the IT security policy, then they can just configure the default user-group either under the parameter-map or on the interface and just have one single global policy configured on the scansafe Tower.

    If they need different policies for different set of peoples, then they can deploy any one of the authentication methods (Webauth, Http-Basic Auth, NLTM) based on their requirements and then configure the scansafe policies based on the user-groups on the Scansafe Tower.

13. Consent-page or Acceptable User Policy (AUP) is supported without any Authentication?

    Yes, AUP is supported without any authentication, So that users just need to accept the consent policies then they are allowed to browse the internet which will be scanned through the scansafe towers.

14. How to pass the username & password securely during authentication?

    Enable ip http secure-server on the ISR-G2, once ip http secure-server CLI is enabled on the ISR-G2, all the transactions between the client and the router/server will be encrypted.

15. Why do I get the certificate warning pages when I enable ip http secure-server command?

    While accessing some HTTPs based websites some of the clients might encounter SSL errors/Certificate warnings because the ISR uses a Test server certificate when ip http secure-server command is enabled. To avoid these SSL errors/Certification warning, please replace the certificate on the ISR-G2 with a certificate signed by a certificate authority that the clients trust in that domain.

16. What's Authentication Order?

    Customer can configure the authentication orders based on their requirements, say for eg: if NTLM fails, then it can trigger the webauth rule once it exceeds the max-login-attempts which is 5 by default.

    Default Authentication order – NTLM, Basic-Auth & Webauth. This default order can be overwritten by ip admission name <rule_name> order command.

17. Difference between NLTM/Http-BASIC Active & passive mode?

    In the Active mode we do user validation and fetch the corresponding user-groups as part of authorization and in case of passive mode we don't do user validation instead we just fetch the user-group as part of authorization from the LDAP server.

18. Multi domain supported with LDAP server?

    No, we support only single domain configuration today.

19. LDAP over SSL is supported on ISR-G2?

    Yes

20. AAA server support for the Auth methods?

    Webauth will work with almost all sorts of authentication servers (RADIUS, TACACS+ , LDAP, Local Authentication)

    Basic-Auth & NTLM supports only LDAP.

21. How to debug content-scan effectively?

    Use conditional debugging for content-scan, where in you can define an ACL and associate to the content-scan debug command which will generate debugs only for the flow which is matching the ACLs, use buffered logging instead of logging console or terminal monitor.

22. AAA Accounting supported for LDAP?

    No, accounting is supported only by RADIUS & TACACS+, so only Webauth can make use of the accounting feature.

23. Support for LDAP Server Failover?

    Yes, We do support LDAP server failover, it picks the LDAP server based on the LDAP server configuration, always the first server is chosen to do user validation and authorization and if it fails it will then failover to the configured Secondary LDAP server and so on,If we have only one LDAP server with no backup, then none of the users will be able to authenticate if the primary LDAP server fails.

24. Nested groups for AD are supported?

    No, Nested Group not supported.

25. How do set Authentication (NTLM/Basic/Webauth) exception?

    We can control only using the ACLs, which is associated to the ip admission rule. We don't support URL/Host/user-agent based exceptions.

26. What are the different types of browser supported/tested for NTLM Authentication?

    NTLM Supported Browsers

    Andriod - ICS4.0.3

    Default Browser

    Mozilla Firefox 14.0.1

    Andriod 2.3.5

    Mozilla Firefox 14.0.1

    Andriod 2.3.4

    Mozilla Firefox 14.0.1

    Andriod 2.2.2

    Mozilla Firefox 14.0.1

    Apple – IPAD2 - IOS 5.1.1

    Safari Browser

    Windows –XP

    IE 6, IE7 & IE8

    Mozilla Firefox 14.0.1

    Windows 7 (64 bit)

    IE 8

    Mozilla Firefox 14.0.1

    Chrome 21.0.1180.89 m

    MAC OS

    Safari Browser

    Windows 7.5 (Mango)

    IE Version 8 (Mobile version)

27. Browsers which supports Transparent NTLM Authentication?

    Internet Explorer & Chrome.

Scansafe Interoperability with other features

1. Scansafe Interoperability Matrix with other features.

    Scansafe doesn't interop with WAAS for the same flow

    Scansafe doesn't interop with CBAC Firewall (But there is a work around which is adding explicit pinholes to the Scansafe Tower IP Address, but recommend Zone Based Firewall with Scansafe)

Scansafe Limitation

1. Today Scansafe can support only 32K Concurrent sessions (Including both HTTP & HTTPs) irrespective of any platform.
2. Header based whitelisting (which includes host & user-agent based whitelisting) wouldn't work if the network has asymmetric routing configured.
3. Some of the Geographic specific services may not work if the scansafe tower doesn't belong to the same geographic region; the workaround is to whitelist such traffic.
4. Host/Header based whitelisting wouldn't work for HTTPs traffic.
5. Scansafe doesn't support VRF
6. Scansafe doesn't support IPV6

Author: Umanath S S (umans@cisco.com)

Date: 25th Sep 2012