Inspection of Database, Directory, and Management Protocols

The following topics explain application inspection for database, directory, and management protocols. For information on why you need to use inspection for certain protocols, and the overall methods for applying inspection, see Getting Started with Application Layer Protocol Inspection.

DCERPC Inspection

DCERPC inspection is not enabled in the default inspection policy, so you must enable it if you need this inspection. You can simply edit the default global inspection policy to add DCERPC inspection. You can alternatively create a new service policy as desired, for example, an interface-specific policy.

The following sections describe the DCERPC inspection engine.

DCERPC Overview

Microsoft Remote Procedure Call (MSRPC), based on DCERPC, is a protocol widely used by Microsoft distributed client and server applications that allows software clients to execute programs on a server remotely.

This typically involves a client querying a server called the Endpoint Mapper listening on a well known port number for the dynamically allocated network information of a required service. The client then sets up a secondary connection to the server instance providing the service. The security appliance allows the appropriate port number and network address and also applies NAT, if needed, for the secondary connection.

The DCERPC inspection engine inspects for native TCP communication between the EPM and client on well known TCP port 135. Map and lookup operations of the EPM are supported for clients. Client and server can be located in any security zone. The embedded server IP address and Port number are received from the applicable EPM response messages. Since a client may attempt multiple connections to the server port returned by EPM, multiple use of pinholes are allowed, which have configurable timeouts.

DCE inspection supports the following universally unique identifiers (UUIDs) and messages:

- End point mapper (EPM) UUID. All EPM messages are supported.
- ISystemMapper UUID (non-EPM). Supported messages are:
  - RemoteCreateInstance opnum4
  - RemoteGetClassObject opnum3
- Any message that does not contain an IP address or port information because these messages do not require inspection.

Configure a DCERPC Inspection Policy Map

To specify additional DCERPC inspection parameters, create a DCERPC inspection policy map. You can then apply the inspection policy map when you enable DCERPC inspection.

Tip You can configure inspection maps while creating service policies, in addition to the procedure explained below. The contents of the map are the same regardless of how you create it.

Procedure

Step 1 Choose **Configuration** > **Firewall** > **Objects** > **Inspect Maps** > **DCERPC**.

Step 2 Do one of the following:

- Click **Add** to add a new map.
- Select a map to view its contents. You can change the security level directly, or click **Customize** to edit the map. The remainder of the procedure assumes you are customizing or adding a map.

Step 3 For new maps, enter a name (up to 40 characters) and description. When editing a map, you can change the description only.

Step 4 In the **Security Level** view of the DCERPC Inspect Map dialog box, select the level that best matches your desired configuration.

If one of the preset levels matches your requirements, you are now done. Just click **OK**, skip the rest of this procedure, and use the map in a service policy rule for DCERPC inspection.

If you need to customize the settings further, click **Details** and continue with the procedure.

Step 5 Configure the desired options.

- **Pinhole Timeout**—Sets the pinhole timeout. Because a client may use the server information returned by the endpoint mapper for multiple connections, the timeout value is configurable based on the client application environment. Range is from 0:0:1 to 1193:0:0.
- **Enforce endpoint-mapper service**—Whether to enforce the endpoint mapper service during binding so that only its service traffic is processed.
- **Enable endpoint-mapper service lookup**—Whether to enable the lookup operation of the endpoint mapper service. You can also enforce a timeout for the service lookup. If you do not configure a timeout, the pinhole timeout is used.

Step 6 Click **OK**.

You can now use the inspection map in a DCERPC inspection service policy.

What to do next

You can now configure an inspection policy to use the map. See Configure Application Layer Protocol Inspection.

GTP Inspection

The following sections describe the GTP inspection engine.

Note GTP inspection requires a special license, which is not supported on all device models. For detailed information, see the tables in the licensing chapter of the general configuration guide.

GTP Inspection Overview

GPRS Tunneling Protocol is used in GSM, UMTS and LTE networks for general packet radio service (GPRS) traffic. GTP provides a tunnel control and management protocol to provide GPRS network access for a mobile station by creating, modifying, and deleting tunnels. GTP also uses a tunneling mechanism for carrying user data packets.

Service provider networks use GTP to tunnel multi-protocol packets through the GPRS backbone between endpoints. In GTPv0-1, GTP is used for signaling between gateway GPRS support nodes (GGSN) and serving GPRS support nodes (SGSN). The GGSN is the interface between the GPRS wireless data network and other networks. The SGSN performs mobility, data session management, and data compression.

You can use the ASA to provide protection against rogue roaming partners. Place the device between the home GGSN and visited SGSN endpoints and use GTP inspection on the traffic. GTP inspection works only on traffic between these endpoints. .

GTP and associated standards are defined by 3GPP (3rd Generation Partnership Project). For detailed information, see http://www.3gpp.org.

Defaults for GTP Inspection

GTP inspection is not enabled by default. However, if you enable it without specifying your own inspection map, a default map is used that provides the following processing. You need to configure a map only if you want different values.

- Errors are not permitted.
- The maximum number of requests is 200.
- The maximum number of tunnels is 500. This is equivalent to the number of PDP contexts (endpoints).
- The GSN timeout is 30 minutes.
- The PDP context timeout is 30 minutes.
- The request timeout is 1 minute.
- The signaling timeout is 30 minutes.
- The tunneling timeout is 1 hour.
- The T3 response timeout is 20 seconds.
- Unknown message IDs are dropped and logged.

  Messages are considered unknown if they are either undefined or are defined in GTP releases that the system does not support.

Configure GTP Inspection

GTP inspection is not enabled by default. You must configure it if you want GTP inspection.

Procedure

Step 1 Configure a GTP Inspection Policy Map, on page 4.

Step 2 Configure the GTP Inspection Service Policy, on page 7.

Step 3 (Optional) Configure RADIUS accounting inspection to protect against over-billing attacks. See RADIUS Accounting Inspection, on page 8.

Configure a GTP Inspection Policy Map

If you want to enforce additional parameters on GTP traffic, and the default map does not meet your needs, create and configure a GTP map.

Before you begin

Some traffic matching options use regular expressions for matching purposes. If you intend to use one of those techniques, first create the regular expression or regular expression class map.

Procedure

Step 1 Choose **Configuration** > **Firewall** > **Objects** > **Inspect Maps** > **GTP**.

Step 2 Do one of the following:

- Click **Add** to add a new map.
- Select a map to view its contents. Click **Customize** to edit the map. The remainder of the procedure assumes you are customizing or adding a map.

Step 3 For new maps, enter a name (up to 40 characters) and description. When editing a map, you can change the description only.

Step 4 In the **Security Level** view of the GTP Inspect Map dialog box, view the current configuration of the map.

The view indicates whether the map uses default values or if you have customized it. If you need to customize the settings further, click **Details**, and continue with the procedure.

Tip The **IMSI Prefix Filtering** button is a shortcut to configure IMSI prefix filtering, which is explained later in this procedure.

Step 5 Click the **Permit Parameters** tab and configure the desired options.

- **Permit Response**—When the ASA performs GTP inspection, by default the ASA drops GTP responses from GSNs that were not specified in the GTP request. This situation occurs when you use load-balancing among a pool of GSNs to provide efficiency and scalability of GPRS.

  To configure GSN pooling and thus support load balancing, create a network object group that specifies the GSNs and select this as a "**From Object Group**." Likewise, create a network object group for the SGSN and select it as the "**To Object Group**." If the GSN responding belongs to the same object group as the GSN that the GTP request was sent to and if the SGSN is in an object group that the responding GSN is permitted to send a GTP response to, the ASA permits the response.

  The network object group can identify the GSN or SGSN by host address or by the subnet that contains them.

- **Permit Errors**—Whether to allow packets that are invalid or that encountered an error during inspection to be sent through the ASA instead of being dropped.

Step 6 Click the **General Parameters** tab and configure the desired options:

- **Maximum Number of Requests**—The maximum number of GTP requests that will be queued waiting for a response.
- **Maximum Number of Tunnels**—The maximum number of active GTP tunnels allowed. This is equivalent to the number of PDP contexts or endpoints. The default is 500. New requests will be dropped once the maximum number of tunnels is reached.
- **Enforce Timeout**—Whether to enforce idle timeouts for the following behaviors. Timeouts are in hh:mm:ss format.
  - GSN—The maximum period of inactivity before a GSN is removed.
  - PDP-Context—The maximum period of inactivity before removing the PDP Context for a GTP session.

- Request—The maximum period of inactivity after which a request is removed from the request queue. Any subsequent responses to a dropped request will also be dropped.
- Signaling—The maximum period of inactivity before GTP signaling is removed.
- T3-Response timeout—The maximum wait time for a response before removing the connection.
- Tunnel—The maximum period of inactivity for the GTP tunnel before it is torn down.

Step 7 Click the **IMSI Prefix Filtering** tab and configure IMSI prefix filtering if desired.

By default, the security appliance does not check for valid Mobile Country Code (MCC)/Mobile Network Code (MNC) combinations. If you configure IMSI prefix filtering, the MCC and MNC in the IMSI of the received packet is compared with the configured MCC/MNC combinations and is dropped if it does not match.

The Mobile Country Code is a non-zero, three-digit value; add zeros as a prefix for one- or two-digit values. The Mobile Network Code is a two- or three-digit value.

Add all permitted MCC and MNC combinations. By default, the ASA does not check the validity of MNC and MCC combinations, so you must verify the validity of the combinations configured. To find more information about MCC and MNC codes, see the ITU E.212 recommendation, *Identification Plan for Land Mobile Stations*.

Step 8 Click the **Inspections** tab and define the specific inspections you want to implement based on traffic characteristics.

a) Do any of the following:
   - Click **Add** to add a new criterion.
   - Select an existing criterion and click **Edit**.

b) Choose the match type for the criteria: **Match** (traffic must match the criterion) or **No Match** (traffic must not match the criterion). Then, configure the criterion:
   - **Access Point Name**—Matches the access point name against the specified regular expression or regular expression class. By default, all messages with valid access point names are inspected and any name is allowed.
   - **Message ID**—Matches the message ID, from 1 to 255. You can specify one value or a range of values. By default, all valid message IDs are allowed.
   - **Message Length**—Matches messages where the length of the UDP payload is between the specified minimum and maximum length.
   - **Version**—Matches the GTP version, from 0 to 255. You can specify one value or a range of values. By default all GTP versions are allowed.

c) For Message ID matching, choose whether to drop the packet or to apply a rate limit in packets per second. The action for all other matches is to drop the packet. For all matches, you can choose whether to enable logging.

d) Click **OK** to add the inspection. Repeat the process as needed.

Step 9 Click **OK** in the GTP Inspect Map dialog box.

You can now use the inspection map in a GTP inspection service policy.

Configure the GTP Inspection Service Policy

GTP inspection is not enabled in the default inspection policy, so you must enable it if you need this inspection. You can simply edit the default global inspection policy to add GTP inspection. You can alternatively create a new service policy as desired, for example, an interface-specific policy.

Procedure

Step 1 Choose **Configuration** > **Firewall** > **Service Policy**, and open a rule.

- To edit the default global policy, select the "inspection_default" rule in the Global folder and click **Edit**.
- To create a new rule, click **Add > Add Service Policy Rule**. Proceed through the wizard to the Rules page.
- If you have a GTP inspection rule, or a rule to which you are adding GTP inspection, select it and click **Edit**.

Step 2 On the Rule Actions wizard page or tab, select the **Protocol Inspection** tab.

Step 3 (To change an in-use policy) If you are editing any in-use policy to use a different inspection policy map, you must disable the GTP inspection, and then re-enable it with the new inspection policy map name:

a) Uncheck the **GTP** check box.
b) Click **OK**.
c) Click **Apply**.
d) Repeat these steps to return to the Protocol Inspections tab.

Step 4 Select **GTP**.

Step 5 If you want non-default inspection, click **Configure**, and do the following:

a) Choose whether to use the default map or to use a GTP inspection policy map that you configured. You can create the map at this time. For detailed information, see Configure a GTP Inspection Policy Map, on page 4.
b) Click **OK** in the Select GTP Inspect Map dialog box.

Step 6 Click **OK** or **Finish** to save the service policy rule.

ILS Inspection

The Internet Locator Service (ILS) inspection engine provides NAT support for Microsoft NetMeeting, SiteServer, and Active Directory products that use LDAP to exchange directory information with an ILS server. You cannot use PAT with ILS inspection because only IP addresses are stored by an LDAP database.

For search responses, when the LDAP server is located outside, consider using NAT to allow internal peers to communicate locally while registered to external LDAP servers. If you do not need to use NAT, we recommend that you turn off the inspection engine to provide better performance.

Additional configuration may be necessary when the ILS server is located inside the ASA border. This would require a hole for outside clients to access the LDAP server on the specified port, typically TCP 389.

Note Because ILS traffic (H225 call signaling) only occurs on the secondary UDP channel, the TCP connection is disconnected after the TCP inactivity interval. By default, this interval is 60 minutes and can be adjusted using the TCP **timeout** command. In ASDM, this is on the **Configuration > Firewall > Advanced > Global Timeouts** pane.

ILS inspection has the following limitations:

- Referral requests and responses are not supported.
- Users in multiple directories are not unified.
- Single users having multiple identities in multiple directories cannot be recognized by NAT.

For information on enabling ILS inspection, see Configure Application Layer Protocol Inspection.

RADIUS Accounting Inspection

The following sections describe the RADIUS Accounting inspection engine.

RADIUS Accounting Inspection Overview

The purpose of RADIUS accounting inspection is to prevent over-billing attacks on GPRS networks that use RADIUS servers. Although you do not need the GTP/GPRS license to implement RADIUS accounting inspection, it has no purpose unless you are implementing GTP inspection and you have a GPRS setup.

The over-billing attack in GPRS networks results in consumers being billed for services that they have not used. In this case, a malicious attacker sets up a connection to a server and obtains an IP address from the SGSN. When the attacker ends the call, the malicious server will still send packets to it, which gets dropped by the GGSN, but the connection from the server remains active. The IP address assigned to the malicious attacker gets released and reassigned to a legitimate user who will then get billed for services that the attacker will use.

RADIUS accounting inspection prevents this type of attack by ensuring the traffic seen by the GGSN is legitimate. With the RADIUS accounting feature properly configured, the ASA tears down a connection based on matching the Framed IP attribute in the Radius Accounting Request Start message with the Radius Accounting Request Stop message. When the Stop message is seen with the matching IP address in the Framed IP attribute, the ASA looks for all connections with the source matching the IP address.

You have the option to configure a secret pre-shared key with the RADIUS server so the ASA can validate the message. If the shared secret is not configured, the ASA will only check that the source IP address is one of the configured addresses allowed to send the RADIUS messages.

Note When using RADIUS accounting inspection with GPRS enabled, the ASA checks for the 3GPP-Session-Stop-Indicator in the Accounting Request STOP messages to properly handle secondary PDP contexts. Specifically, the ASA requires that the Accounting Request STOP messages include the 3GPP-SGSN-Address attribute before it will terminate the user sessions and all associated connections. Some third-party GGSNs might not send this attribute by default.

Configure RADIUS Accounting Inspection

RADIUS accounting inspection is not enabled by default. You must configure it if you want RADIUS accounting inspection.

Procedure

Step 1 Configure a RADIUS Accounting Inspection Policy Map, on page 9.

Step 2 Configure the RADIUS Accounting Inspection Service Policy, on page 10.

Configure a RADIUS Accounting Inspection Policy Map

You must create a RADIUS accounting inspection policy map to configure the attributes needed for the inspection.

Procedure

Step 1 Choose **Configuration** > **Firewall** > **Objects** > **Inspect Maps** > **RADIUS Accounting**.

Step 2 Do one of the following:

- Click **Add** to add a new map.
- Select a map and click **Edit**.

Step 3 For new maps, enter a name (up to 40 characters) and description. When editing a map, you can change the description only.

Step 4 Click the **Host Parameters** tab and add the IP addresses of each RADIUS server or GGSN.

You can optionally include a secret key so that the ASA can validate the message. Without the key, only the IP address is checked. The ASA receives a copy of the RADIUS accounting messages from these hosts.

Step 5 Click the **Other Parameters** tab and configure the desired options.

- **Send responses to the originator of the RADIUS accounting message**—xxWhether to mask the banner from the ESMTP server.
- **Enforce user timeout**—Whether to implement an idle timeout for users, and the timeout value. The default is one hour.

- **Enable detection of GPRS accounting**—Whether to implement GPRS over-billing protection. The ASA checks for the 3GPP VSA 26-10415 attribute in the Accounting-Request Stop and Disconnect messages in order to properly handle secondary PDP contexts. If this attribute is present, then the ASA tears down all connections that have a source IP matching the User IP address on the configured interface.
- **Validate Attribute**—Additional criteria to use when building a table of user accounts when receiving Accounting-Request Start messages. These attributes help when the ASA decides whether to tear down connections.

  If you do not specify additional attributes to validate, the decision is based solely on the IP address in the Framed IP Address attribute. If you configure additional attributes, and the ASA receives a start accounting message that includes an address that is currently being tracked, but the other attributes to validate are different, then all connections started using the old attributes are torn down, on the assumption that the IP address has been reassigned to a new user.

  Values range from 1-191, and you can enter the command multiple times. For a list of attribute numbers and their descriptions, see http://www.iana.org/assignments/radius-types.

Step 6 Click **OK**.

You can now use the inspection map in a RADIUS accounting inspection service policy.

Configure the RADIUS Accounting Inspection Service Policy

RADIUS accounting inspection is not enabled in the default inspection policy, so you must enable it if you need this inspection. Because RADIUS accounting inspection is for traffic directed to the ASA, you must configure it as a management inspection rule rather than a standard rule.

Procedure

Step 1 Choose **Configuration** > **Firewall** > **Service Policy**, and open a rule.

- To create a new rule, click **Add > Add Management Service Policy Rule**. Proceed through the wizard to the Rules page.
- If you have a RADIUS accounting inspection rule, or a management rule to which you are adding RADIUS accounting inspection, select it, click **Edit**, and click the **Rule Actions** tab.

Step 2 (To change an in-use policy) If you are editing any in-use policy to use a different inspection policy map, you must disable the RADIUS accounting inspection, and then re-enable it with the new inspection policy map name:

a) Select **None** for the RADIUS Accounting map.
b) Click **OK**.
c) Click **Apply**.
d) Repeat these steps to return to the Protocol Inspections tab.

Step 3 Choose the desired **RADIUS Accounting Map**. You can create the map at this time. For detailed information, see Configure a RADIUS Accounting Inspection Policy Map, on page 9.

Step 4 Click **OK** or **Finish** to save the management service policy rule.

RSH Inspection

RSH inspection is enabled by default. The RSH protocol uses a TCP connection from the RSH client to the RSH server on TCP port 514. The client and server negotiate the TCP port number where the client listens for the STDERR output stream. RSH inspection supports NAT of the negotiated port number if necessary.

For information on enabling RSH inspection, see Configure Application Layer Protocol Inspection.

SNMP Inspection

SNMP application inspection lets you restrict SNMP traffic to a specific version of SNMP. Earlier versions of SNMP are less secure; therefore, denying certain SNMP versions may be required by your security policy. The ASA can deny SNMP versions 1, 2, 2c, or 3. You control the versions permitted by creating an SNMP map.

SNMP inspection is not enabled in the default inspection policy, so you must enable it if you need this inspection. You can simply edit the default global inspection policy to add SNMP inspection. You can alternatively create a new service policy as desired, for example, an interface-specific policy.

Procedure

Step 1 Choose **Configuration** > **Firewall** > **Objects** > **Inspect Maps** > **SNMP**.

Step 2 Click **Add**, or select a map and click **Edit**. When adding a map, enter a map name.

Step 3 Select the SNMP versions to disallow.

Step 4 Click **OK**.

What to do next

You can now configure an inspection policy to use the map. See Configure Application Layer Protocol Inspection.

SQL*Net Inspection

SQL*Net inspection is enabled by default. The inspection engine supports SQL*Net versions 1 and 2, but only the Transparent Network Substrate (TNS) format. Inspection does not support the Tabular Data Stream (TDS) format. SQL*Net messages are scanned for embedded addresses and ports, and NAT rewrite is applied when necessary.

The default port assignment for SQL*Net is 1521. This is the value used by Oracle for SQL*Net, but this value does not agree with IANA port assignments for Structured Query Language (SQL). If your application uses a different port, apply the SQL*Net inspection to a traffic class that includes that port.

Note Disable SQL*Net inspection when SQL data transfer occurs on the same port as the SQL control TCP port 1521. The security appliance acts as a proxy when SQL*Net inspection is enabled and reduces the client window size from 65000 to about 16000 causing data transfer issues.

For information on enabling SQL*Net inspection, see Configure Application Layer Protocol Inspection.

Sun RPC Inspection

This section describes Sun RPC application inspection.

Sun RPC Inspection Overview

Sun RPC protocol inspection is enabled by default. You simply need to manage the Sun RPC server table to identify which services are allowed to traverse the firewall. However, pinholing for NFS is done for any server even without the server table configuration.

Sun RPC is used by NFS and NIS. Sun RPC services can run on any port. When a client attempts to access a Sun RPC service on a server, it must learn the port that service is running on. It does this by querying the port mapper process, usually rpcbind, on the well-known port of 111.

The client sends the Sun RPC program number of the service and the port mapper process responds with the port number of the service. The client sends its Sun RPC queries to the server, specifying the port identified by the port mapper process. When the server replies, the ASA intercepts this packet and opens both embryonic TCP and UDP connections on that port.

NAT or PAT of Sun RPC payload information is not supported.

Manage Sun RPC Services

Use the Sun RPC services table to control Sun RPC traffic based on established Sun RPC sessions.

Procedure

Step 1 Choose **Configuration** > **Firewall** > **Advanced** > **SUNRPC Server**.

Step 2 Do one of the following:

- Click **Add** to add a new server.
- Select a server and click **Edit**.

Step 3 Configure the service properties:

- **Interface Name**—The interface through which traffic to the server flows.
- **IP Address/Mask**—The address of the Sun RPC server.
- **Service ID**—The service type on the server. To determine the service type (for example, 100003), use the **sunrpcinfo** command at the UNIX or Linux command line on the Sun RPC server machine.

- **Protocol**—Whether the service uses TCP or UDP.
- **Port/Port Range**—The port or range of ports used by the service.
- **Timeout**—The idle timeout for the pinhole opened for the connection by Sun RPC inspection.

Step 4 Click **OK**.

Step 5 (Optional.) Monitor the pinholes created for these services.

To display the pinholes open for Sun RPC services, enter the **show sunrpc-server active** command. Select **Tools** > **Command Line Interface** to enter the command. For example:

```
hostname# show sunrpc-server active
LOCAL FOREIGN SERVICE TIMEOUT
-----------------------------------------------
1 209.165.200.5/0 192.168.100.2/2049 100003 0:30:00
2 209.165.200.5/0 192.168.100.2/2049 100003 0:30:00
3 209.165.200.5/0 192.168.100.2/647 100005 0:30:00
4 209.165.200.5/0 192.168.100.2/650 100005 0:30:00
```

The entry in the LOCAL column shows the IP address of the client or server on the inside interface, while the value in the FOREIGN column shows the IP address of the client or server on the outside interface.

If necessary, you can clear these services using the **clear sunrpc-server active**

XDMCP Inspection

XDMCP is a protocol that uses UDP port 177 to negotiate X sessions, which use TCP when established.

For successful negotiation and start of an XWindows session, the ASA must allow the TCP back connection from the Xhosted computer. To permit the back connection, you can use access rules to allow the TCP ports. Alternatively, you can use the **established** command on the ASA. Once XDMCP negotiates the port to send the display, the **established** command is consulted to verify if this back connection should be permitted.

During the XWindows session, the manager talks to the display Xserver on the well-known port 6000 | n. Each display has a separate connection to the Xserver, as a result of the following terminal setting.

```
setenv DISPLAY Xserver:n
```

where *n* is the display number.

When XDMCP is used, the display is negotiated using IP addresses, which the ASA can NAT if needed. XDCMP inspection does not support PAT.

For information on enabling XDMCP inspection, see Configure Application Layer Protocol Inspection.

VXLAN Inspection

Virtual Extensible Local Area Network (VXLAN) inspection works on VXLAN encapsulated traffic that passes through the ASA. It ensures that the VXLAN header format conforms to standards, dropping any

malformed packets. VXLAN inspection is not done on traffic for which the ASA acts as a VXLAN Tunnel End Point (VTEP) or a VXLAN gateway, as those checks are done as a normal part of decapsulating VXLAN packets.

VXLAN packets are UDP, normally on port 4789. This port is part of the default-inspection-traffic class, so you can simply add VXLAN inspection to the inspection_default service policy rule. Alternatively, you can create a class for it using port or ACL matching.

History for Database, Directory, and Management Protocol Inspection

Feature Name	Releases	Feature Information
DCERPC inspection support for ISystemMapper UUID message RemoteGetClassObject opnum3.	9.4(1)	The ASA started supporting non-EPM DCERPC messages in release 8.3, supporting the ISystemMapper UUID message RemoteCreateInstance opnum4. This change extends support to the RemoteGetClassObject opnum3 message. We did not modify any ASDM screens.
VXLAN packet inspection	9.4(1)	The ASA can inspect the VXLAN header to enforce compliance with the standard format. We modified the following screen: **Configuration > Firewall > Service Policy Rules > Add Service Policy Rule > Rule Actions > Protocol Inspection**.