coservit

Intelligent insight software

coservit
ServiceNav

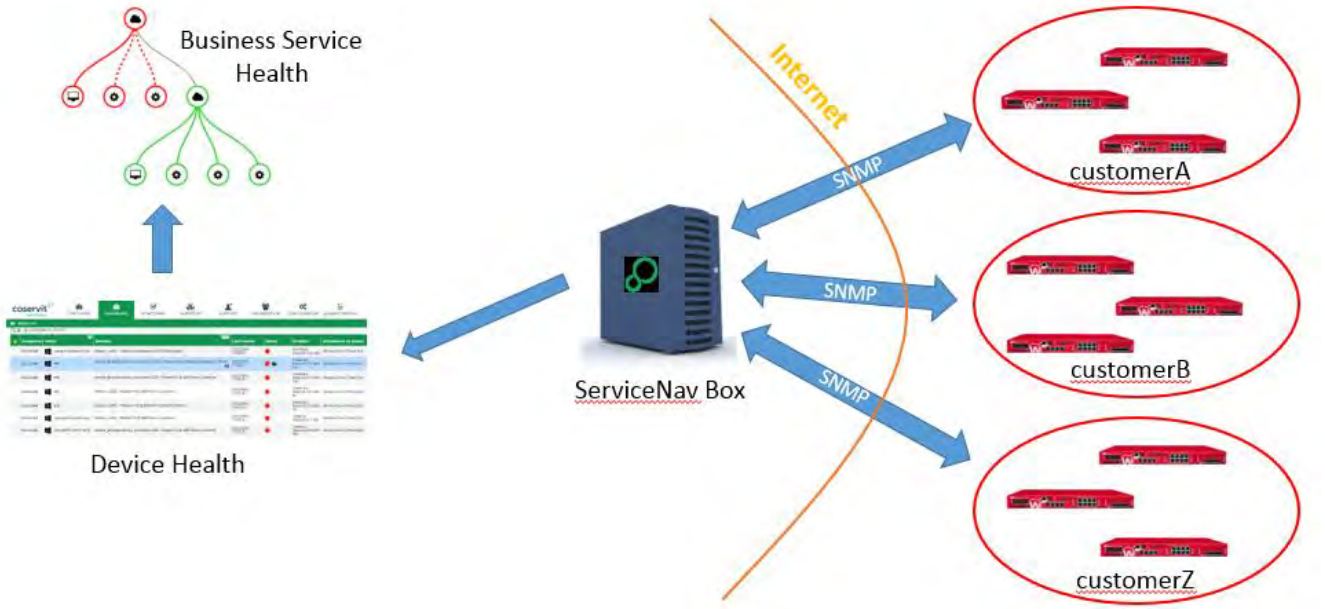
ServiceNav integration with WatchGuard Solutions

More information: ServiceNav
Email: info@coservit.com

ServiceNav from Coservit is a service monitoring and reporting solution proven in the MSP space. By collecting KPI's from devices in a typical IT environment, ServiceNav reports on the availability of business services in real-time.

ServiceNav – WatchGuard – MSPs

How to ensure you collect the most relevant information to create compelling stories to attract prospects. With a ServiceNav Monitoring Box installed in the MSPs datacentre, all WatchGuard services at all customer sites can be monitored, using SNMP, from that single Box:



Configuration

ServiceNav has pre-built checkpoints for monitoring and reporting (via SNMP) a variety of metrics specific to WatchGuard appliances:

Metric	Description
WatchGuard-Active-Tunnels	Retrieves the number of active IPSEC tunnels on a WatchGuard XTM host and compares this number with the argument supplied. Goes to CRITICAL if the number of tunnels is different.
WatchGuard-Monitor-Tunnel	Monitors the status of the IPSEC tunnel whose endpoint IP address is specified as an argument. Goes to CRITICAL where the tunnel is not active.

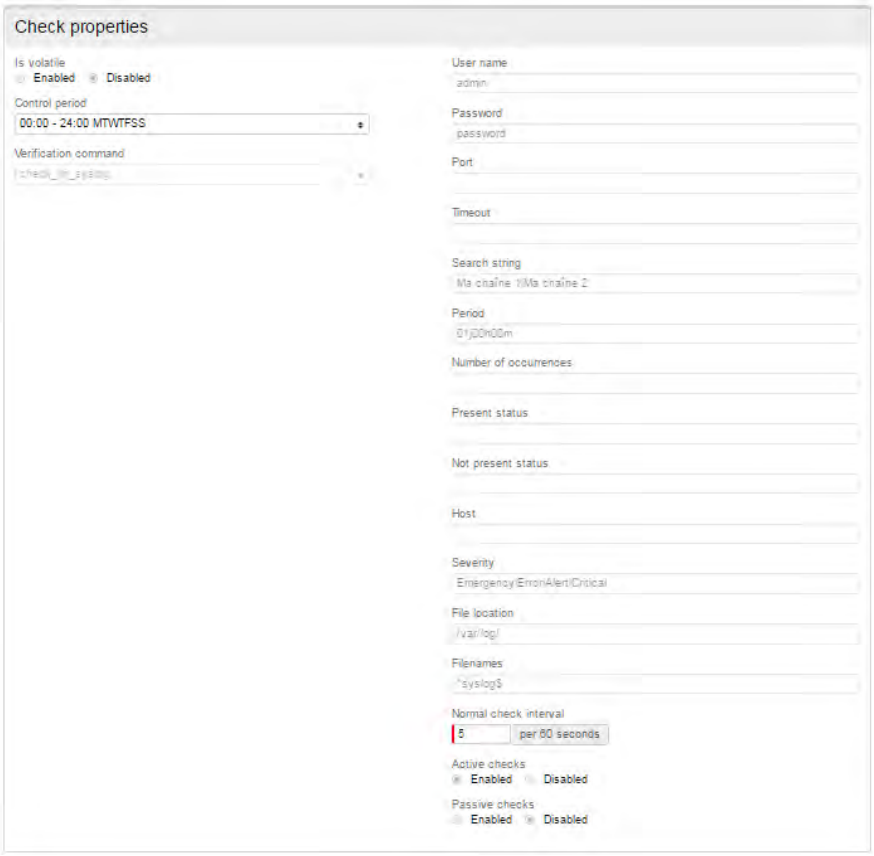
WatchGuard-XCS-Inodes	Monitors the percentage of inodes (indexes) used by the host on each partition. Goes to ALERT if the specified threshold is exceeded for at least one of the partitions, goes to CRITICAL if the specified threshold is exceeded for at least one of the partitions.
WatchGuard-XCS-Mail-Clean	Retrieves the volume of e-mail messages virus-free or not identified as unsolicited e-mail over a given period (hourly, daily, weekly). Goes to ALERT if the set threshold is exceeded, goes to CRITICAL if the set threshold is exceeded.
WatchGuard-XCS-Mail-Deferred	Retrieves the number of delayed messages. Goes to ALERT if the set threshold is exceeded, goes to CRITICAL if the set threshold is exceeded.
WatchGuard-XCS-Mail-Disk	Monitors disk space used by each of the host's partitions. Goes to ALERT if the specified threshold is exceeded for at least one of the partitions, goes to CRITICAL if the specified threshold is exceeded for at least one of the partitions.
WatchGuard-XCS-Mail-Queued	Retrieves the number of messages queued. Goes to ALERT if the set threshold is exceeded, goes to CRITICAL if the set threshold is exceeded.
WatchGuard-XCS-Mail-Ram	Retrieves the total percentage of memory used by the host. Goes to ALERT if the set threshold is exceeded, goes to CRITICAL if the set threshold is exceeded.
WatchGuard-XCS-Mail-Received	Retrieves the volume of e-mail messages received over a given time period (hourly, daily, weekly). Goes to ALERT if the set threshold is exceeded, goes to CRITICAL if the set threshold is exceeded.
WatchGuard-XCS-Mail-Rejected	Retrieves the volume of e-mail messages rejected over a given time period (hourly, daily, weekly). Goes to ALERT if the set threshold is exceeded, goes to CRITICAL if the set threshold is exceeded.
WatchGuard-XCS-Mail-Sent	Retrieves the volume of e-mail messages sent over a given time period (hourly, daily, weekly). Goes to ALERT if the set threshold is exceeded, goes to CRITICAL if the set threshold is exceeded.
WatchGuard-XCS-Mail-Spam	the number of e-mail messages flagged as SPAM over a given period (hourly, daily, weekly). Goes to ALERT if the set threshold is exceeded, goes to CRITICAL if the set threshold is exceeded.
WatchGuard-XCS-Mail-Virus	Retrieves the number of e-mail messages with a virus detected over a given period (hourly, daily, weekly). Goes to ALERT if the set threshold is exceeded, goes to CRITICAL if the set threshold is exceeded.

ServiceNav permits the bundling up of such checkpoints into “host templates” that allow for rapid, consistent bulk-deployments to multiple WatchGuard devices.

WatchGuard Logging

The ServiceNav Monitoring Box has a built in syslog server that can be specified in WatchGuard device configurations as a logging destination.

ServiceNav's syslog checkpoint can be configured to alert based on specific strings, or severities encountered in log entries:



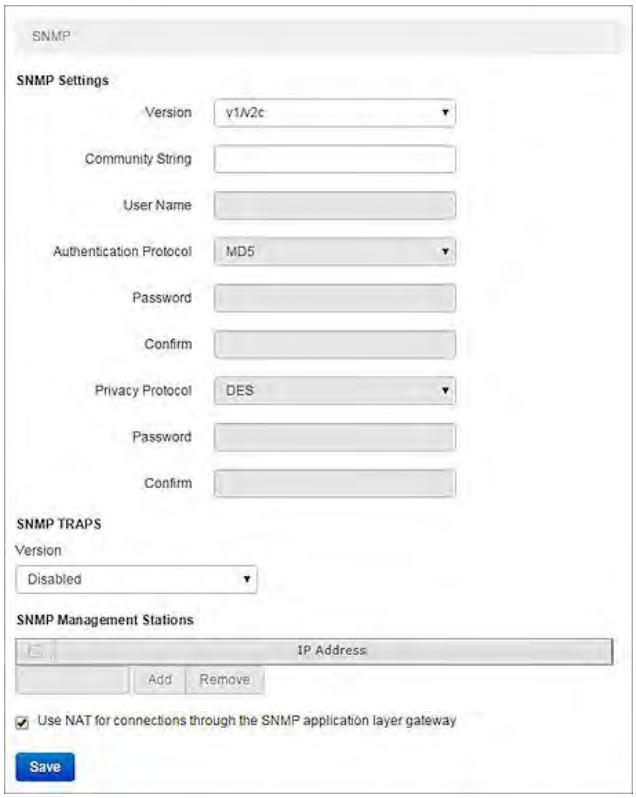
The syslog messages can report on both functional and hardware health.

Configuring Watchguard for ServiceNav monitoring via SNMP

The simplest approach to monitoring XTM and XCS devices is to configure them to accept polls from an SNMP server (in this case the ServiceNav monitoring box).
To enable SNMP polling, from the Fireware Web UI:

1. Select System → SNMP.

   The SNMP page appears.



2. To enable SNMP, from the **Version** drop-down list, select an option:

    - v1/v2c
        - Type the **Community String** the SNMP server uses when it contacts the device. The community string is used as a user ID or password that allows access to the statistics of a device.
    - v3
        - Type the **User Name** the SNMP server uses when it contacts the device.
        - If your SNMP server uses authentication, from the **Authentication Protocol** drop-down list, select **MD5** or **SHA1**.
        - In the adjacent **Password** and **Confirm** text boxes, type the authentication password.

3. To enable NAT for all SNMP connections through your Firebox, select the **Use NAT for connections through the SNMP application layer gateway** check box.
4. Click **Save**.

To enable your Firebox to receive SNMP polls, you must also add an SNMP packet filter policy.

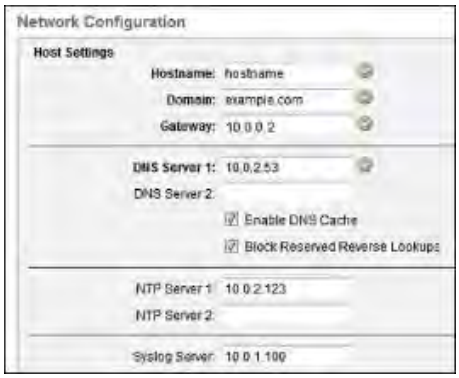
1. Select **Firewall > Firewall Policies**.
2. Click **Add Policy**.
3. From the **Packet Filters** drop-down list, select **SNMP**. Click **Add Policy**.
   The Policy Configuration page appears.
4. In the **From** section, click **Add**.
   The Add Member dialog box appears.
5. From the **Member type** drop-down list, select **Host IP**.
6. In the **Member type** text box, type the IP address of your SNMP server. Click **OK**.
   The IP address of the SNMP server appears in the From list.
7. From the **From** list, select **Any-Trusted**. Click **Remove**.
8. In the **To** section, click **Add**.
   The Add Member dialog box appears.
9. From the drop-down list, select **Firebox**. Click **OK**.
   Firebox appears in the To list.
10. From the **To** list, select **Any-External**. Click **Remove**.
11. Click **Save**

Configuring Watchguard XCS for ServiceNav monitoring via Syslog

You can forward all of the system's log files to a syslog server that collects and stores log files from many sources. The syslog files can then be analyzed by a separate logging and reporting program (in our case, interrogated by ServiceNav checkpoints)
Syslog includes these system logs: Mail log, System log, Auth log, and cron messages.

To define a syslog host:

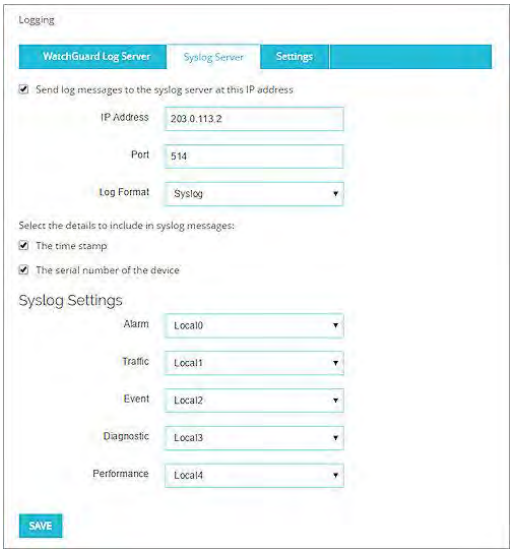
1. Select **Configuration > Network > Interfaces**.
2. Type the IP address or host name of the ServiceNav box in the **Syslog Server** field.



3. Click **Apply**.

Configuring Watchguard XTM for ServiceNav monitoring via Syslog

1. Select **System > Logging**.
   The Logging page appears.
2. Select the **Syslog Server** tab.
3. Select the **Send log messages to the syslog server at this IP address** check box.
4. In the **IP Address** text box, type the IP address for the ServiceNav Box.
5. In the **Port** text box, the default syslog server port (514) appears. To change the server port, type or select a different port for your server.
6. From the **Log Format** drop-down list, select **Syslog**.
   The details available to include in the log messages depend on the log format you select.



The **Syslog Settings** for the syslog log format.

7. To include the date and time that the event occurs on your Firebox in the log message details, select the **The time stamp** check box.
8. To include the serial number of the Firebox in the log message details, select the **The serial number of the device** check box.
9. In the **Syslog Settings** section, for each type of log message, select a syslog facility from the drop-down list.
    - For high-priority syslog messages, such as alarms, select **Local0**.
    - To assign priorities for other types of log messages (lower numbers have greater priority), select **Local1**–**Local7**.
    - To not send details for a message type, select **NONE**.
10. Click **Save**.