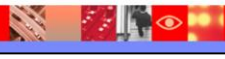

IBM
IBM Tivoli® Training
IBM Tivoli Monitoring 6.1
Communication Ports and Firewalls
Tivoli software
ON DEMAND BUSINESS
© 2006 IBM Corporation

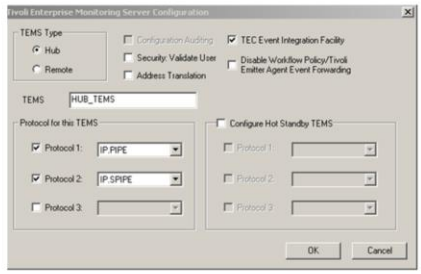
Objectives

- Upon completion of this module, you should be able to:
  - Describe the communications protocols used by IBM Tivoli Monitoring 6.1.
  - List the default and required ports.
  - Describe the requirements for deploying IBM Tivoli Monitoring 6.1 with a firewall.



Communication – Protocol Support

- Multiple Protocols supported
  - IP.PIPE (TCP)
    - Connection-oriented transport layer to provide reliable, sequenced stream data delivery
  - IP.SPIPE (SSL over TCP)
  - IP.UDP (UDP)
    - Provide application programs with a best efforts connectionless datagram delivery service
    - Perceived to be insecure
  - SNA
- TEMS support for up to three protocols at the same time
- Warehouse Proxy–RPC for data transfer from agents and TEMS

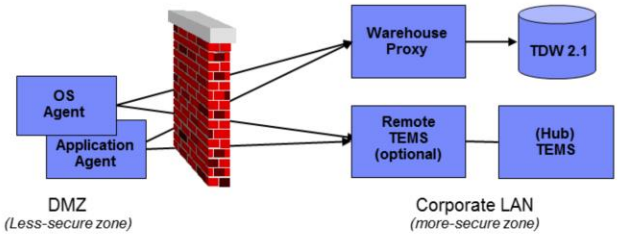


Port Requirements - Infrastructure

- Agents, remote TEMSs, and the TEP server: port 1918/TCP to hub TEMS
  - Agents: -- TCP--> remote TEMS:1918
  - Remote TEMS: -- TCP --> hub TEMS:1918
  - TEPS: -- TCP --> hub TEMS:1918
- Browser clients: 1920 by default to TEP server
  - Browser: -- TCP --> TEPS:1920, Browser: -- TCP --> TEPS:15001
  - Desktop: -- TCP --> TEPS:1920, Desktop: -- TCP --> TEPS:15001
- TEC Port opened on firewall if between HUB TEMS and TEC Server
  - Hub TEMS: -- TCP --> TEC:5529
- Miscellaneous
  - Default port for SSL communication is 3660/TCP (instead of 1918/TCP).
  - The TEMS can also be configured to use 1920/UDP.
  - Ports can be changed, although it is advised to use the defaults.
  - If the variable **IP POOL** is set in the configuration file then the RPC code will request from the OS a specific port number which by default will be a well known port. It will request all numbers in the specified port range. In cases where the **IP POOL** is not specified then it is the responsibility of the OS to return any unused ephemeral port.

Deploying in Firewall environments

- Agents connecting to their hub or remote TEMS can be a concern in DMZs.
- When data collection occurs at the agent, additional communication to the Warehouse Proxy needs to be established.
  - In these cases, collection at the TEMS might be an alternative.



- NAT is supported through Partition Files.
- Application Security: The TEMS does not accept commands from agents. Only sampling data is accepted by the TEMS.
- Support is provided for Unidirectional Communication and Relay Function

Port Requirements - Agents

- The **Universal Agent** (UA) can be configured for communications over a variety of ports. Here are typical ports used by the Universal Agent:
  - Port 161 Standard SNMP port (used when running SNMP UA)
  - Port 1919 Data Clearing House port
  - Port 7500 Socket Data Provider listening port
  - Port 7575 Post Data Provider listening port
  - Port 7600 API Data Provider listening port
  - Port 7700-7710 Console ports (one for each DP that is activated at startup)
- **Other agents** have application-specific requirements, such as:
  - Port 1414 IBM MQ Series
  - SAP RFC Agent for SAP R/3
  - ...

Copyright and trademark information