



Mel Farber

**A Practical Guide to monitoring systems in a DMZ
by OpenView Operations for Unix**

Hewlett-Packard

© 2004 Hewlett-Packard Development Company, L.P.
The information contained herein is subject to change without notice





Acknowledgements

Stefan Bergstein

Dave Trout



Topics

- Terminology
- Challenges and issues with past solutions
- Alternatives
- Benefits of this solution
- DCE daemonless communication
- DCE daemonless communication using SSH
- How we did it
- Security
- Questions

What is OpenView?

- OpenView is a suite of products for monitoring and managing networked devices and systems
 - Monitoring
 - Management
 - Presentation
- Network Management
 - Network Node Manager
- System Management
 - OpenView Operations for UNIX/Windows (OVOU/OVOW)
- Performance Management
 - Coda, Performance Agent, Performance Manager, GlancePlus
- Reporting and Presentation
 - Reporter, Service Information Portal

System Management through OpenView Operations (OVO)



- Enterprise system monitoring and management
 - OVOU for mostly UNIX environment
 - OVOW for mostly Windows environment
 - Basic and advanced system management
 - Trap receiver (NNM, devices, 3rd parties)
 - OVO agents messages and threshold exceptions
 - Processes placed on monitored systems
 - Communication through RPC (**NOT SNMP**)
 - Agent runs independent of server status

System Management through OpenView Operations (OVO)



- Enterprise system monitoring and management
 - Monitors log file for errors
 - Monitors performance metric exceptions
 - Monitors for scripted exceptions
 - File system usage, processes not running, etc.
 - Advanced monitoring using HP Smart Plug-Ins
 - Collection of pre-defined templates/policies that monitor for log file errors, performance exceptions, scripted exceptions – Databases, Remedy, Network, Active Directory, etc.

What is an Agent?

- Collection of processes placed on a device or a system to enhance remote monitoring and access
- SNMP agent (standard agent used on all devices and most general purpose systems)
- Private agents
 - Defined and installed by management applications, such as OpenView

System Management through OpenView Operations (OVO)

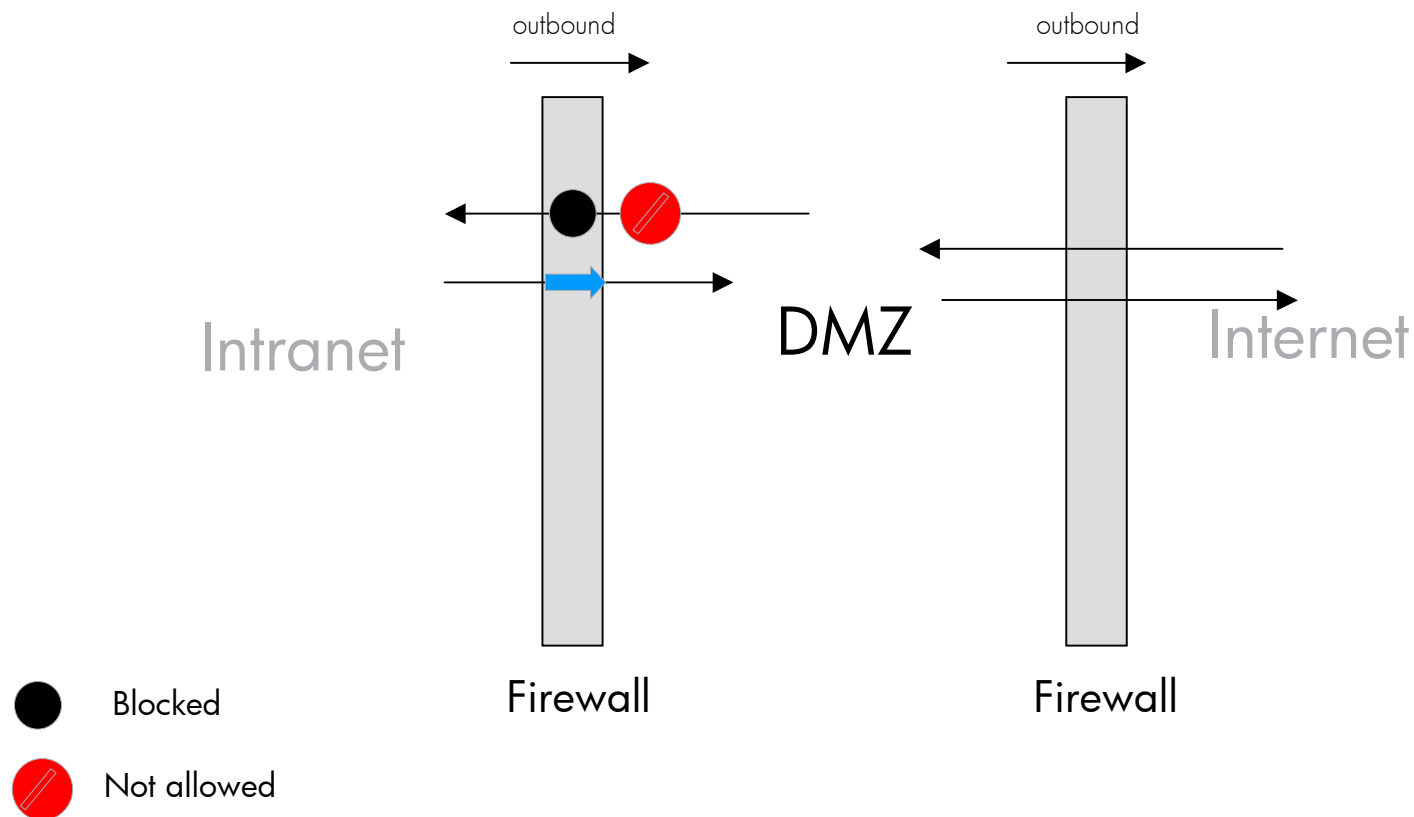


- Server <-> Agent communication
 - Server can be HP-UX or Solaris
 - Agents available for HP-UX, Tru64, VMS, Solaris, Linux, Windows, AIX and SGI
 - Agents are installed from the server onto the target host
 - Agent communicates back to one or more servers
 - exceptions (agents are not polled) as defined by configuration elements called templates or policies
 - Metric thresholds exceeded
 - Messages
 - Scheduled actions (centrally controlled cron capability)
 - Traps received

What is a DMZ?

- Area between an organization's intranet and the internet
- Area where an organization's web/application servers are available to customer's or interested parties
- Organizations maintain 2 firewalls
 - Between the internet and the DMZ
 - Between the DMZ and the intranet (protected area)

Network view Intranet->DMZ-Internet



What is SSH?

- Secure Shell is a program for logging into a remote machine and for executing commands on a remote machine. It replaces telnet, rlogin and rsh to provide secure encrypted communications between two untrusted hosts. X11 connections and **arbitrary TCP/IP ports** can also be forwarded over the secure channel.
- SSH2 is the sequel to the SSH1 protocol.
- SCP is the companion capability for securely copying between systems

What is DCE?

- The OSF Distributed Computing Environment (DCE) is an industry-standard, vendor-neutral set of distributed computing technologies. DCE is deployed in critical business environments by a large number of enterprises worldwide. It is a mature product with three major releases, and is the only middleware system with a comprehensive security model.

What is DCE?

- DCE provides a complete Distributed Computing Environment infrastructure. It provides security services to protect and control access to data, name services that make it easy to find distributed resources, and a highly scalable model for organizing widely scattered users, services, and data. DCE runs on most major computing platforms and is designed to support distributed applications in heterogeneous hardware and software environments. DCE is a key technology in three of today's most important areas of computing: security, the World Wide Web and distributed objects.
- Methodology has been superceded by lighter weight protocols

Security issues with DCE

- DCE uses port 135, which is attacked by blaster worm
- Ports used to communicate between two systems is typically negotiated between the systems
- Ports are not fixed



Challenges in monitoring systems in the DMZ

- Protect network from attacks by worms, viruses and hackers
- Vulnerability to the internal network of systems and devices
- Balance need for monitoring and need to maintain strict security
- Organizational lines of responsibility

Issues for monitoring systems in the DMZ

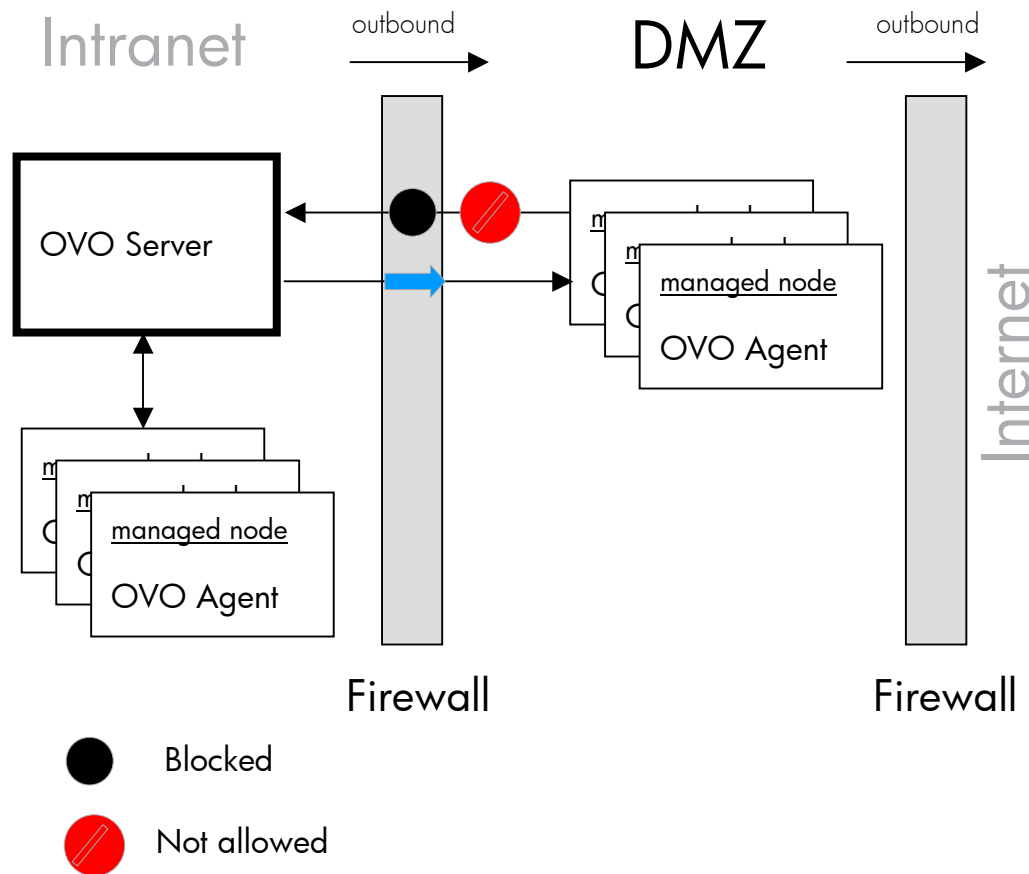


- Inbound communication (agent initiates communication)
- Multiple rules in the Firewall
- Limited ability to quickly break the link to the DMZ

Alternative Solutions

- Static port definition rejected 
 - Lots of pre-defined ports
 - Potential vulnerability
- Mgmt. Server inside the DMZ rejected 
 - Complex, maintenance nightmare
 - No ability to run applications from main OVO Server
- Pre-defined DCE rules in firewall rejected 
 - Checkpoint rules specific for OpenView Operations
 - Requires DCE port 135 out to DMZ

Server <-> Agent Communication



outbound only

- Organization does not allow any inbound connections into the Intranet
- Firewall administrators don't open any inbound ports.

OVO agent

- Message agent sends messages and output from remote applications
- Distribution agent requests configuration information from the management server
- Both are inbound connections because the agent initiates the communication

objective

- Get rid of the inbound connection by using the DCE daemon-less feature and SSH port forwarding
- Fully functional agent

Benefits of using SSH for agent communication



- Incorporates DCE daemonless communication (no use of port 135)
- Outbound-only server to agent communication
- Requires only a single firewall rule change
- Get SSH Functionality and Security
- Tunneling / port forwarding (well known and well trusted)
 - Network security
 - Strong authentication
 - Public key cryptography
 - Password authentication
 - Host authentication
 - Data encryption

Pre-requisites for this solution

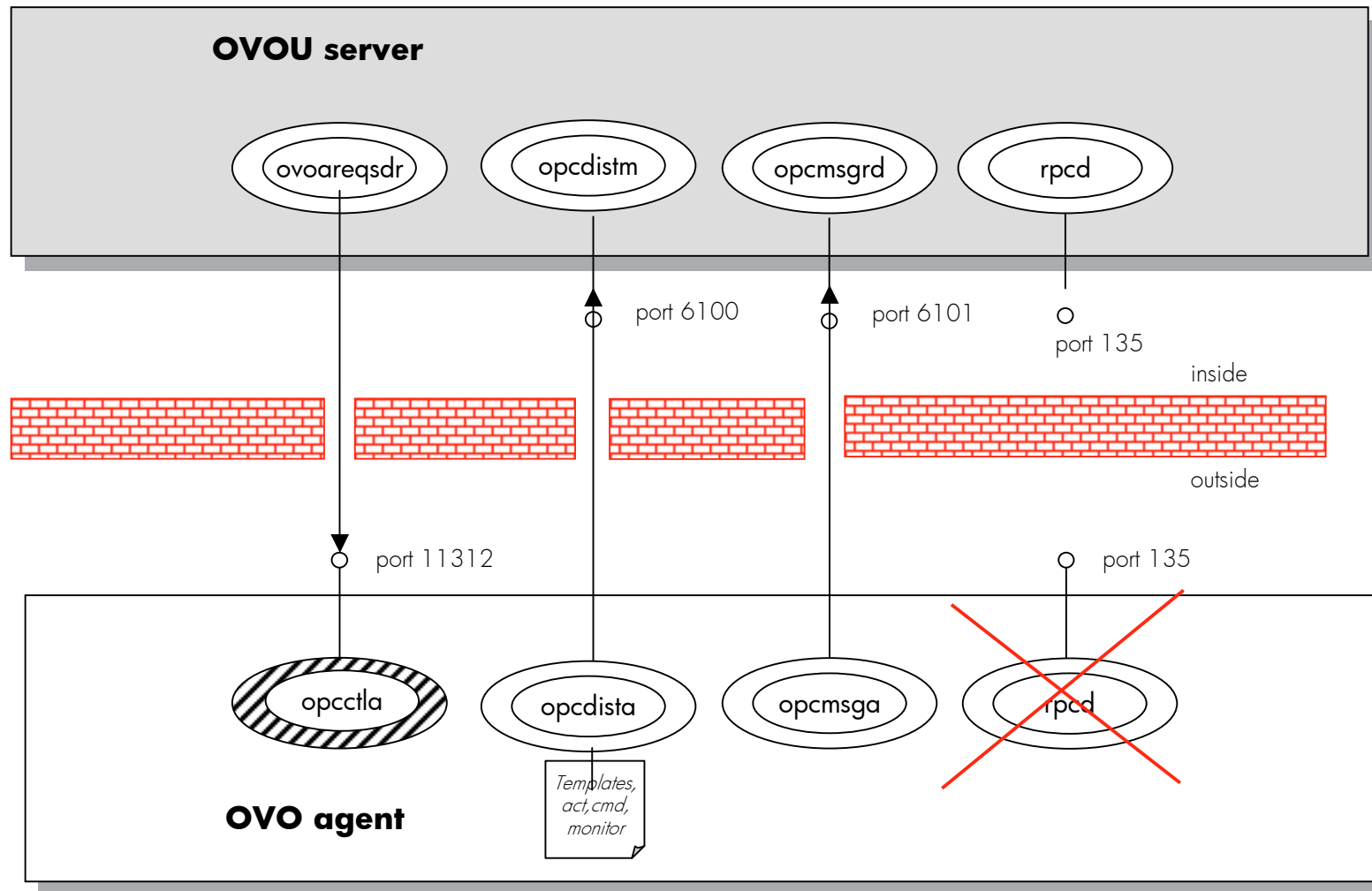
- SSH2 on all participating systems
- Firewall must allow outbound SSH communication
- Firewall must allow outbound communication for a single TCP port
- DMZ nodes must support DCE communication
- Scripts to start, stop and monitor SSH tunnels
- To access OpenView Operations performance data two additional ports need to be opened in the firewall

OVO DCE Daemonless Communication



- No use of port 135
- OpenView Operations for UNIX Server
 - message receiver and distribution manager each use one pre-defined inbound port
 - request sender communicates to agent using only one outbound port
- OpenView Operations for UNIX Agent
 - no endpoint mapper on agent (i.e., DCE daemon is not running)
 - control agent is using one pre-defined outbound port
 - message and distribution agent can communicate directly to server using one inbound port per agent
- Full Functionality
 - start action, tools (applications), start/stop/status of agent, deliver messages, action status, annotations, remote policy/instrumentation deployment

OVO DCE Daemonless Communication



OVO configuration changes

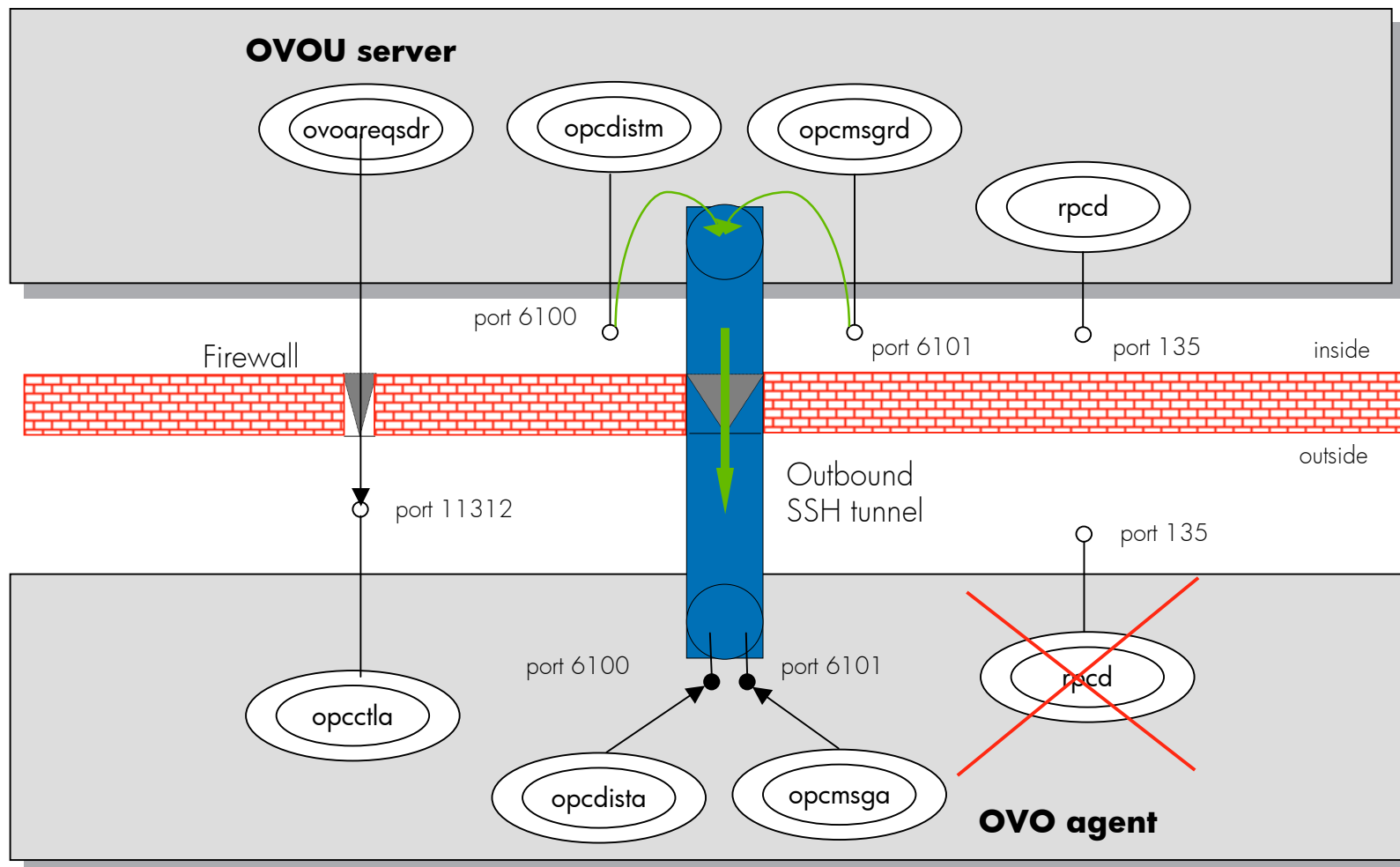
- OVO Server Configuration
 - Define the ports to be used by the server to communicate to the agent
- OVO Agent Configuration
 - Define the ports to be used by the agent to communicate to the server

OVO Communication with SSH Tunneling



- Everything remains the same as w/o SSH, with noted exceptions
- OVO Server
 - No changes
- OVO Agent
 - Port opened in firewall allows the control agent to communicate to the server using one pre-defined outbound port
 - Agent processes use two SSH tunnels to communicate back to the server

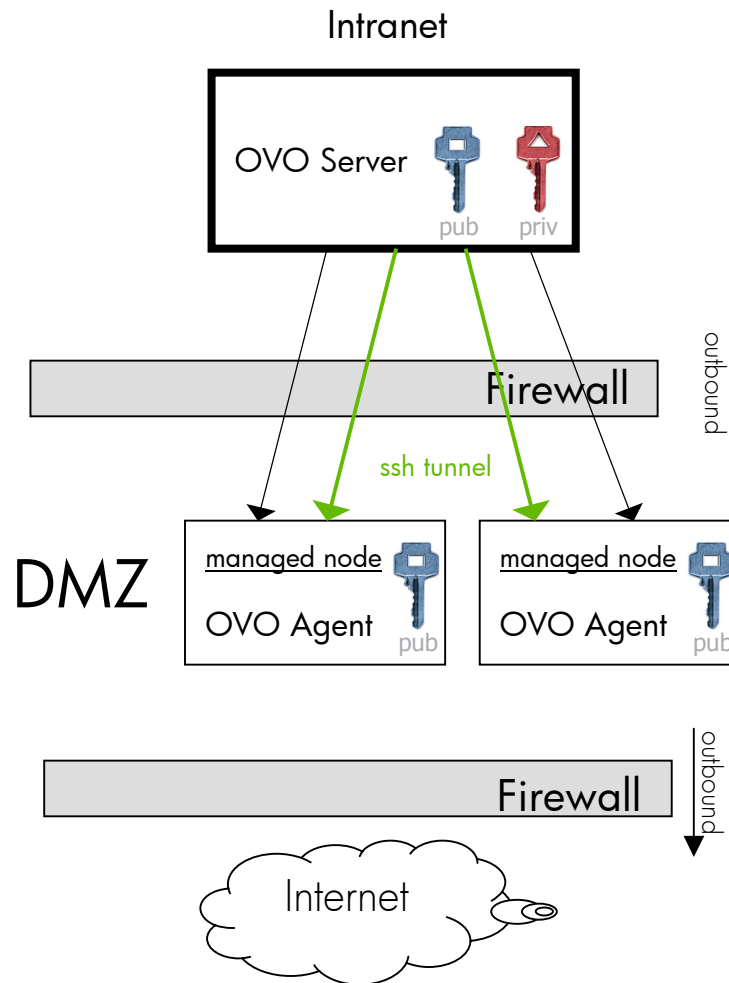
OVO Communication with SSH Tunneling



Configuration changes

- OVO Server Configuration does **NOT** change
- OVO Agent Configuration changes slightly
 - The configuration references the remote system's own loopback address (127.0.0.1) instead of the actual IP address of the management server

OVO Communication with SSH



Server Configuration File

NO CHANGES

Agent Configuration File

**OPC_RESOLVE_IP 127.0.0.1
OPC_DIST_MODE DIST_RPC
OPC_RPC_ONLY TRUE**

How we did it

- Open firewall for TCP port from inside to outside
- Ensure firewall allows ssh from inside to outside
- Ensure ssh configuration allows for port forwarding
- Create a user on each target system and on the management server
 - User shell should be /bin/false on target system
 - User shell is for a regular user on the management server
- Install OVO agent as usual and edit configuration files
- Disable DCE startup on node

We used scp to copy the installation files and did a manual install

We created file snippets to edit configuration files and startup file

How we did it

- Create and exchange user keys so that the designated user on the OVO server can log into the managed node without entering a password
 - Create user keys on the management server (once per management server)
 - Copy public keys to the target system

We had multiple management servers so we created a single file with all the keys and copied that to the node

How we did it

- Set file and directory permissions (600/700)
- Log into node from server as dmz_user to dmz_user
 - Sets known_hosts file entry on management server

We had multiple servers so we copied the known_hosts files to each server

How we did it

- SSH command
 - `ssh -N -n $node -R 6100:$OVO_SERVER:6100 -R 6101:$OVO_SERVER:6101 >/export/home/dmz_user/$SNAME.status 2>&1 &`
- Save PID
 - `echo $! > /export/home/dmz_user/$SNAME.pid`

We created a script (invokessh.sh) to do all the work

We had a script to start the SSH sessions for designated nodes

We had a script to kill the SSH sessions for designated nodes

How we did it

- Maintaining the configuration
 - Use a file with a list of nodes for DMZ nodes
 - Create start, stop and monitor scripts for SSH sessions
 - Monitor syslog on target for failed tunnels
 - Monitor status files on server for failures and failed tunnels and restart SSH if necessary (check for too many restarts in a time span)

We created an OVO Scheduled action (cron functionality) to keep the tunnel from timing out

We used a file for our list of DMZ nodes (easier to create and maintain and we could comment out troublesome nodes)

We used the PID files to check for the SSH processes running and to kill SSH sessions

How we did it

- Responsible manager configuration
 - A responsible manager configuration defines which messages go to which manager
 - A responsible manager configuration defines which OVO servers can distribute software or run commands
 - A system configured in this process uses a slightly different syntax than intranet systems

We created a script to create a responsible manager file for each DMZ node

How we did it

- Switching primary managers
 - The agent will **ALWAYS** forward messages to the system running the SSH tunnel.

Cannot run applications from other than the OVO server that initiated the SSH tunnels!!

Cannot send some messages to one server and some to another.

Follow the sun could work if the SSH sessions followed the sun.

How we did it



- Configuration capabilities
 - All typical capabilities were tested to be fully functional in this new environment

How we did it

- **Be nice to security people** (they have their responsibilities and they can do nasty things to your big plans)
- Management Server Security
 - IDS software
 - SSH configuration for user invoking the SSH session
 - File permissions and ownership
- Managed node Security
 - IDS software
 - SSHD configuration
 - /bin/false for user shell
 - File permissions and ownership



Questions



HP WORLD 2004

Solutions and Technology Conference & Expo

Co-produced by:



RECOMMENDED TRAINING VENUE FOR THE
HP Certified Professional

