An Evaluation of Firewall Configuration Methods

S P Maj, W Makasiranondh, D Veal,

Edith Cowan University, Perth, Western Australia

Summary
Firewalls are essential aspects of all networks. However they are complex and if not correctly configured and managed may result in security breaches. The traditional text-based Command Line Interface is a powerful but difficult tool to use. It is inherently sequential requiring multiple commands. Web-based Graphical User interfaces are progressively being deployed such as the Cisco Security Device Manager. With features such as AutoSecure it is possible to automatically generate device configuration code. Furthermore firewall implementation is relatively simple with configuration code again being automatically generated. However, the code generated may well be substantial. Successful management of secure devices requires the network administrator to be able to understand how the different protocols are interacting in order to be able to successfully conduct fault diagnosis. This paper demonstrates how State Model Diagrams can be a useful management tool for firewall management.

Key words:
Firewall, Security Device Manager, State Model Diagrams.

1. Introduction

Security is an essential aspect of network configuration and management. However, a network will typically consist of many different user applications all of which represent potential security breaches. Furthermore there are numerous protocols such as Packet assembler/disassembler (PAD), Internet Control Message Protocol (ICMP) and Simple Network Management Protocol (SNMP) that are enabled by default and must be explicitly disabled. Whilst other protocols such as HTTP and HTTPs must be allowed but restricted using access control lists. It is essential therefore to disable a potentially wide range of services and devices interfaces that are not being used but selectively restrict other protocols with an appropriate firewall configuration.

After identifying potential security breaches a router must be configured by means of a firewall. Firewalls were initially simple ACLs. However there now a range of different ACLs that include: standard, extended, reflexive, dynamic, time based and more advanced security implementations such as Context Based Access Control and Zone Based firewalls. A firewall employs directional, rule-based stateful packet analysis for traffic from both low security zones to high security zones and vice versa.

Context-based access control (CBAC) is a solution available within the Cisco Internetwork Operating System (IOS) Firewall. CBAC provides stateful Application Layer filtering and is able to securely monitor multimedia applications and protocols that require multiple channels for communication, such as FTP and H.323. However CBAC are potentially complex to implement. In order to address this problem Zone Based Policy Firewall (ZBF or ZPF or ZFW) technology was introduced. Whilst there are advantages to using ZBF its implementation and management is still complex.

2. User Interfaces

Regardless of which security protocol is employed, correct device and protocol configuration is of paramount importance. According to Bartal,

"This is a crucial task … The bottom line, however, is that the security of the whole intranet depends upon the exact content of the rule-base, with no level of abstraction available. Since the syntax and semantics of the rules and their ordering depend upon the firewall product/vendor, this is akin to the dark ages of software, where programs were written in assembly language so that the programmer had to know all the idiosyncrasies of the target processor." [1]

Furthermore security devices and protocols are complex systems. According to Van den Akker,

"Other security breaches caused by user error can be attributed to the complexity of modern systems. Users must be able to use and clearly understand the system in order to use it effectively." [2]

Network devices were traditionally configured and managed using the text-based Command Line Interface (CLI). This is a powerful tool but the output is verbose and complex. One small typographical error could result in a potential security breach. According to Shultz,

"People, for example, are almost invariably involved in installing, configuring and maintaining technology, something that leave ample opportunity for human error that can result in exposures that can allow those who are

Manuscript received August 5, 2010
Manuscript revised August 20, 2010

intent on evildoing to bypass or defeat this technology." [3]

Nielson developed criteria for a successful human interface [4]. In order to address the specific concerns of security Johnston proposed a security Human Computer Interface (HCI-S) [5]. HCI-S criteria are:

- Convey features
- Visibility of system status
- Learn ability
- Aesthetic and minimalist design
- Errors
- Satisfaction
- Trust

Web-based Graphical User interfaces are designed to control complexity and are progressively being deployed. Cisco the world's largest vendor of network equipment, now recommend this use of the Security Devices Manager (SDM) GUI. Using the SDM it is possible to identify all devices interfaces in use; identify protocol vulnerabilities with the associated recommended actions. The option exists to generate and download the appropriate device configurations. In addition to this a feature called AutoSecure can be used to lock down router management and forwarding plane services. The router management plane is concerned with all devices management services and functions such as password encryption, legal banner notifications, etc. The forwarding plane is responsible for packet switching and functions include traffic filtering using Access Control Lists (ACLs) and firewall based protocols. AutoSecure is typically used to define the baseline security policy on new devices. Further security enhancements would then be implemented based on specific organizational requirements. The SDM provides a simple to use 'tick box' GUI with automatic configuration code generation.

The SDM also provides a firewall status monitor that can be used for simple fault diagnosis. However more complex problems require the network administrator to revert to using the CLI with its associated complexities. An alternative method of security device configuration and management is State Model Diagrams (SMDs).

2. State Model Diagrams

State Model Diagrams (SMDs) can be used to selectively extract and integrate relevant output from the CLI [6]. SMDs are modular and hierarchical. Hence they can be used to provide leveling by means of top-down decomposition. Using SMDs a complex network may be documented and navigated. Individual devices may be selected and increasing levels of protocol detail may be obtained whilst maintaining contextual links [7]. SMDs can be used to model all network devices (routers, switches, wireless access points) and a wide range of associated protocols. Furthermore it has been demonstrated that SMDs can be used to model dedicated Private Internet Exchange (PIX) firewalls and also implementations of the Internet Protocol Security (IPSec) standard [8]. Significantly a single SMD represents the output from multiple CLI commands. This is important because it is then possible to concurrently view and analyze configuration details and protocol state interactions [9]. Using the SMD run-time model it is possible to validate network and protocol behavior in real-time.

A Zone-Based Firewall was implemented using these three different methods: Security Devices Manager (SDM), Command Line Interface (CLI) and State Model Diagrams (SDM) and the results evaluated.

3. Security Device Manager – ZBF configuration

Regardless of which configuration method is employed when configuring a router with a Zone Based Firewall there are five steps:

1. Create zones
2. Define traffic classes
3. Define firewall policies
4. Assign policy maps to zone-pairs
5. Assign router interfaces to zones.

There are two SDM deployment methods – SDM Wizard and SDM Manual.

The initial SDM wizard screen allows the user to select either basic or advanced firewall configuration. The basic firewall option applies pre-defined rules suitable for the most common modes of attack. The SDM provides a screen that allows the user to define which interface is high security and which is low security. If the interfaces are not already configured to be operational the option exists to enable that interface. After the interfaces are selected the user is provided with a 'slider' option that can be moved from high to low security. As the slider is moved an associate text box indicates the protocols affected. It is possible to preview the associated configurations for each level of security. After the appropriate level of security is selected configuration code is automatically generated and downloaded to the router. It should be noted that even for the low security option over 100 lines of configuration code are generated.

The advanced firewall option allows the user to apply either pre-defined rules or user defined rules. The same ‘slider’ option is available (figure 1). Again configuration code is automatically downloaded to the router.

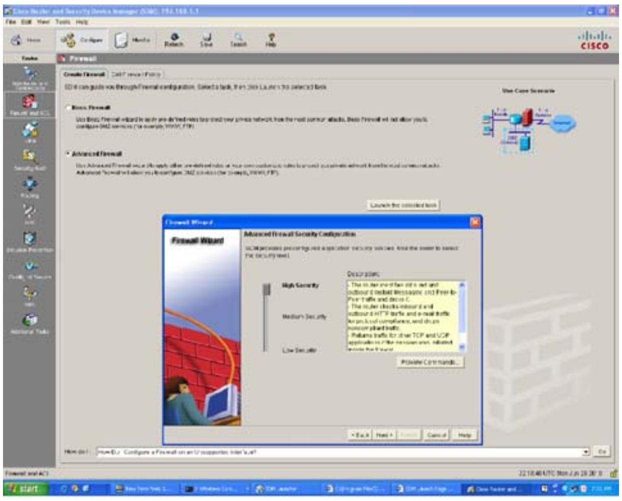

Cisco Router and Security Device Manager (SDM): 192.168.1.1
Firewall Wizard
Advanced Firewall Security Configuration
High Security
Medium Security
Low Security

Fig. 1 Advanced Firewall configuration screen in Cisco Security Device Manager (SDM)

For both the basic and advanced options, after the configuration is downloaded it is possible to view and edit the firewall policy (figure 2).

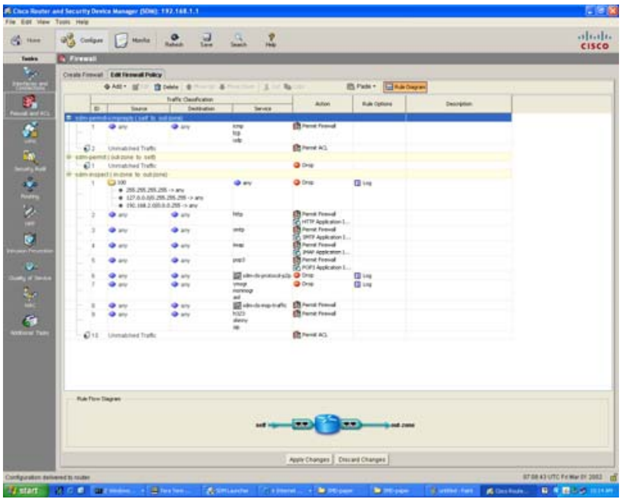


Fig. 2 SDM Edit Firewall Policy

The SDM manual option provides the user with greater configuration control. For example when configuring a class map it is possible to construct a class map from a menu of different protocol options (figure 3).

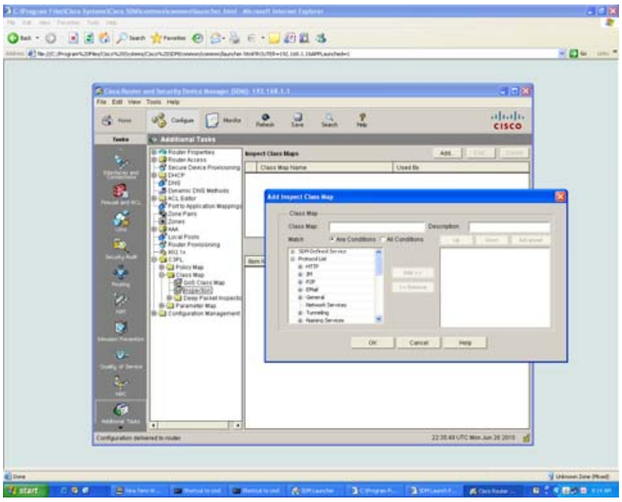


Fig. 3 SDM Manual – Inspect Class Map

Similarly policy map protocol inspection actions can be individually configured (figure 4).

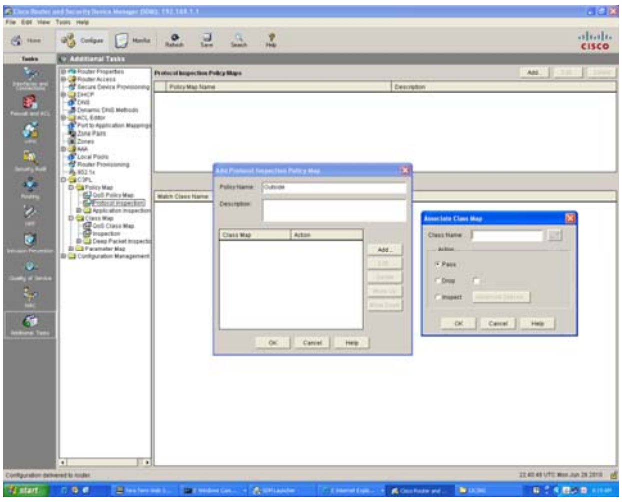
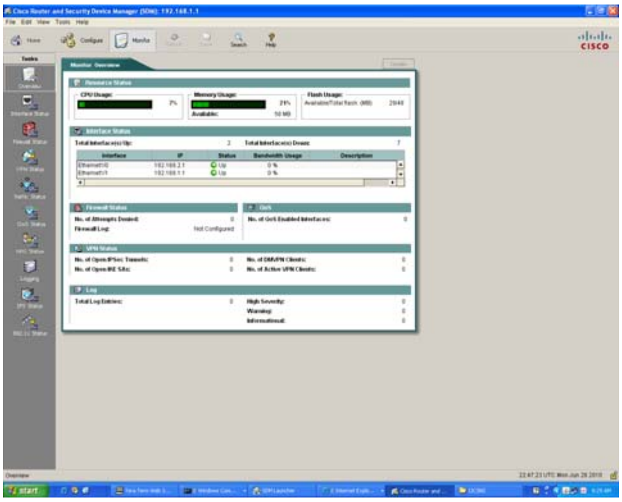

Cisco Router and Security Device Manager (SDM): 192.168.1.1
Additional Tasks
Protocol Inspection Policy Maps
Add Protocol Inspection Policy Map
Associate Class Map
Pass
Drop
Inspect
OK
Cancel
Help

Fig. 4 SDM Manual – Policy map inspection

SDM provides a device monitor overview that operates in real time (figure 5). This allows the overall status of the device to be monitored.

It is also possible to monitor the firewall activity for each zone pair that is configured on the device (figure 6). Packet activity for a zone pair can be selectively monitored in real-time.


Cisco Router and Security Device Manager (SDM): 192.168.1.1
File Edit View Tools Help
Home
Configure
Monitor
Search
Help
Monitor Overview

Resource Status

CPU Usage: 7%

Memory Usage: 21%
Available: 50 MB

Flash Usage:
Available/Total flash (MB) 2048

Interface Status

Total Interface(s) Up: 2 Total Interface(s) Down: 7

Interface	IP	Status	Bandwidth Usage	Description
Ethernet1/0	192.168.2.1	Up	0 %	
Ethernet1/1	192.168.1.1	Up	0 %	

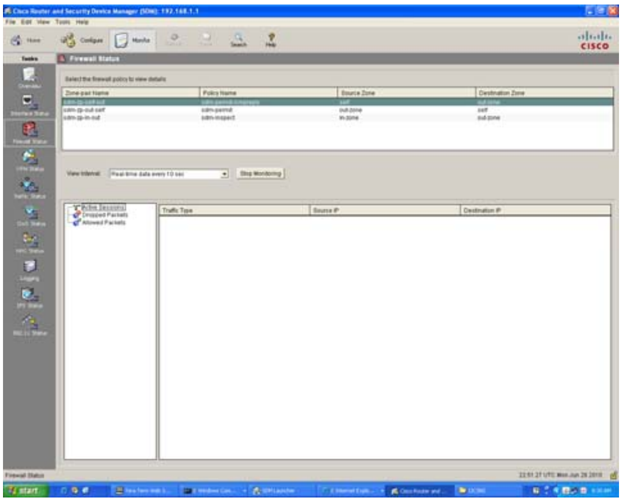
Firewall Status
No. of Attempts Denied: 0
Firewall Log: Not Configured

QoS
No. of QoS Enabled Interfaces: 0

VPN Status
No. of Open IPSec Tunnels: 0
No. of Open IKE SAs: 0
No. of DMVPN Clients: 0
No. of Active VPN Clients: 0

Log
Total Log Entries: 0
High Severity: 0
Warning: 0
Informational: 0

Fig. 5 SDM Resource Status Monitor



Select the firewall policy to view details

Zone-pair Name	Policy Name	Source Zone	Destination Zone
sdm-zp-self-out	sdm-permit-icmpreply	self	out-zone
sdm-zp-out-self	sdm-permit	out-zone	self
sdm-zp-in-out	sdm-inspect	in-zone	out-zone

View Interval: Real-time data every 10 sec

Traffic Type	Source IP	Destination IP

Fig. 6 SDM Firewall status monitor

4. Command Line Interface – ZBF configuration

The CLI requires the user to enter text-based configuration commands. The CLI interface is hierarchical and certain commands can only be entered in specific contexts. For example to configure an interface to be in a specific zone it is necessary to change to that interface context as follows:

```
Router(config)#interface Ethernet 1/1
Router(config-if)#zone-member security INSIDE
```

Assuming zones have been created (INSIDE – high security, OUTSIDE – low security). ZBF traffic classes are created as follows. Note, selection options are provided by “?”.

```
Router(config)#class-map ?
    WORD       class-map name
    match-all  Logical-AND all matching statements
    match-any  Logical-OR all matching statements
    type       type of the class-map

Router(config)#class-map type ?
     access-control   access-control specific class-map
     control          Configure a control policy class-map
     inspect          Configure CBAC Class Map
     logging          Class map for control-plane packet logging
     port-filter      Class map for port filter
     queue-threshold  Class map for queue threshold
     stack            class-map for protocol header stack specification

Router(config)#class-map type inspect ?
     WORD       class-map name
     aol        Configure CBAC class-map for IM-AOL protocol
     edonkey    eDonkey
     fasttrack  FastTrack Traffic – KaZaA ...
     gnutella   Gnutella Version2 Traffic - BearShare ...
     http       Configure CBAC class-map for HTTP protocol
     imap       Configure CBAC class-map for IMAP protocol
     kazaa2     Kazaa Version 2
     match-all  Logical-AND all matching statements
     match-any  Logical-OR all matching statements
     msnmsgr    Configure CBAC class-map for IM-MSN
     pop3       Configure CBAC class-map for POP3 protocol
     smtp       Configure CBAC class-map for SMTP protocol
     sunrpc     Configure CBAC class-map for RPC protocol
     ymsgr      Configure CBAC class-map for IM-YAHOO

Router(config)#class-map type inspect OUT ?
     <cr>

Router(config)#class-map type inspect OUT
Router(config-cmap)#?
    Class-map configuration commands:
     description  Class-Map description
     exit         Exit from class-map configuration mode
     match        classification criteria
     no           Negate or set default values of a command
     rename       Rename this class-map

Router(config-cmap)#match ?
     access-group  Access group
     class-map     Class map
     protocol      PAM Protocol

Router(config-cmap)#match access-group 100
Router(config-cmap)#end
```

The resultant class map is as follows:

```
!
class-map type inspect match-all OUT
    match access-group 100
!
```

After completing all the five steps to create a ZBF the resultant router configuration is as follows:

```
!
class-map type inspect match-all OUT
       match access-group 100
!
policy-map type inspect INOUT
        class type inspect OUT
         inspect
        class class-default
!
zone security INSIDE
zone security OUTSIDE
zone-pair security INOUT source INSIDE destination OUTSIDE
        service-policy type inspect INOUT
!
interface Ethernet1/0
        no ip address
        zone-member security OUTSIDE
        shutdown
        half-duplex
!
interface Ethernet1/1
        no ip address
        zone-member security INSIDE
        shutdown
        half-duplex
!
access-list 100 permit ip 192.168.1.0 0.0.0.255 any
!
```

In order to evaluate the operational status of the ZBF it is necessary to enter the following CLI command.

```
Router#show policy-map type inspect zone-pair session
```

To determine the operational status of the router requires numerous other commands such as:

```
Router#show interface e1/0

Router#show ip route

Router#show arp
```

In effect it is not possible to monitor the operational status of the device in real time.

5. State Model Diagrams – ZBF configuration

SMD based device configuration is implemented by means of tables. Each table clearly defines independent but closely coupled ZBF functional groups: access-list; class-map; policy-map and zone-pair. Correct configuration mandates that the field of each functional group is correctly matched.

The initial SMD is the high level topology map (Figure 7). A topology map defines the overall network architecture and includes: devices, interfaces, IP addresses and connections.

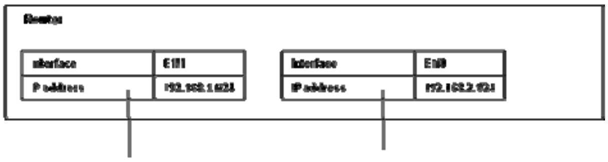


Fig. 7 State Model Diagram (SMD) topology map

In this case there is only one device – Router. It is possible to select this device and progressively obtain more details. For example the router has a routing table, Address Resolution table and Zone Based Firewall table (figure 8).

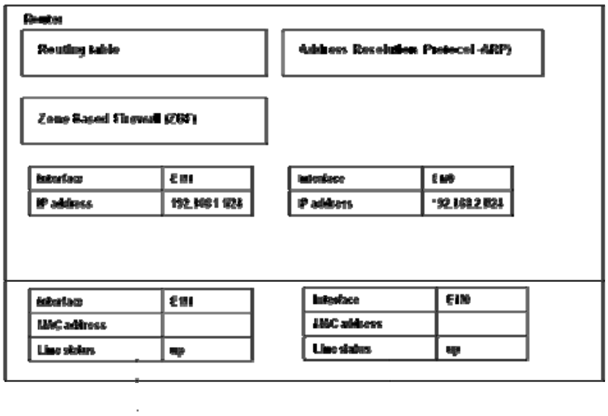
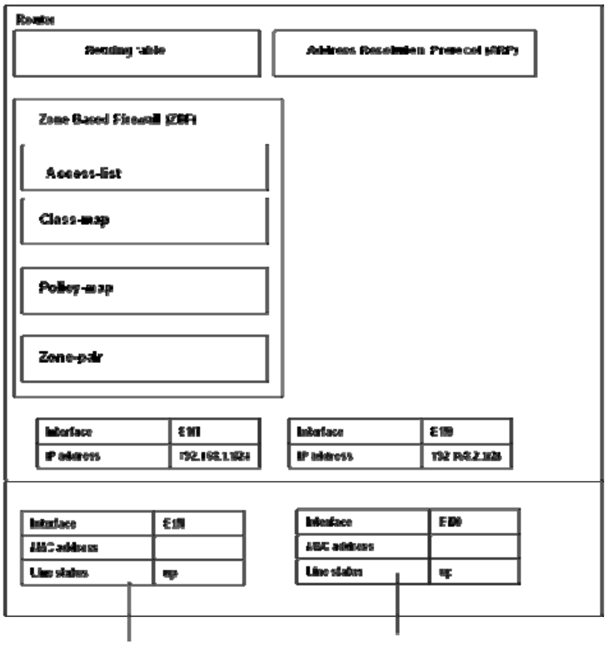


Fig. 8 SMD diagram after expanding layer 3 information

The ZBF table can be expanded to show the four functional groups (figure 9). In order to obtain further details and ensure a single screen footprint it is possible to selectively close tables (figure 10).

The SMD software uses a combination of Simple Network Management Protocol (SNMP) and PING to automatically populate the tables. SNMP is a client-server protocol with three components: managed device, software agent and a network manager. The software agent on the router automatically gathers specific data about device status in order to populate Management Information Bases (MIBs). The network manger interrogates the MIBs. Hence it is possible to use the SMD software to detect not only configuration errors but also run-time errors in real-time. For example, should an interface change to the down state (for whatever reason), the Line protocol status for that interface will change color. Unlike other network management tools the SMD software allows the user can specify: table columns, table names and color schemes for error conditions.

Significantly the SMD allows the user the ability to monitor not only the ZBF protocol implementation but also all other protocols operational on the device in real time.



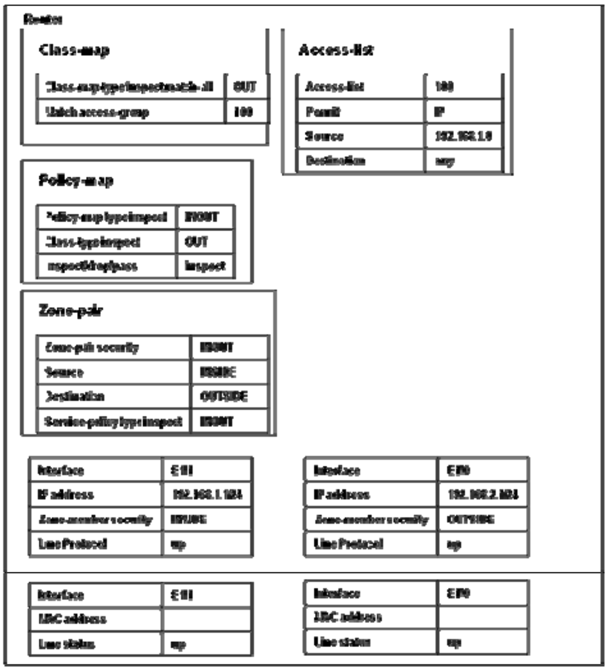
Interface	E1/1
IP address	192.168.1.1/24

Interface	E1/0
IP address	192.168.2.1/24

Interface	E1/1
MAC address	
Line status	up

Interface	E1/0
MAC address	
Line status	up

Fig. 9 SMD displaying security related content of the Firewall



Class-map type inspect match-all	OUT
Match access-group	100

Access-list	100
Permit	IP
Source	192.168.1.0
Destination	any

Policy-map type inspect	INOUT
Class-type inspect	OUT
Inspect/drop/pass	inspect

Zone-pair security	INOUT
Source	INSIDE
Destination	OUTSIDE
Service-policy type inspect	INOUT

Interface	E1/1
IP address	192.168.1.1/24
Zone-member security	INSIDE
Line Protocol	up

Interface	E1/0
IP address	192.168.2.1/24
Zone-member security	OUTSIDE
Line Protocol	up

Interface	E1/1
MAC address	
Line status	up

Interface	E1/0
MAC address	
Line status	up

Fig. 10 SMD diagram displaying detailed information of security related features

3. Conclusions

The CLI is a powerful method of device configuration but is syntactically demanding. Furthermore it is not possible to monitor device status in real-time. The CLI is represents one extreme of the HCI-S criteria i.e. high trust and minimalistic but difficult to learn. However fault diagnosis for an experienced CLI user will be much simpler.

Some of the problems associated with the complex text based CLI can be addressed by using web-based GUIs such as the Security Device Manager (SDM). The SDM Wizard is easy to use and can automatically generate device configuration code. However the SDM Wizard decouples the administrator from the detail necessary to understand the interaction between protocols and the protocol states. Furthermore using this option substantial configuration code is generated even for the simplest level of firewall security. Arguably automatically generated code may be more complex during fault diagnosis. The Manual SDM provides greater granularity of control. Whilst this represents a more complex configuration option the user is more directly responsible for configuration code generation. The SDM therefore provides a provides different configuration modes ranging from almost entirely automatic with minimal input from the user to one in which the user is able to make menu based selections for each of the five steps in firewall configuration. Furthermore SDM provides options to monitor both device status and firewall operation in real-time.

The SMD method user interface represents an intermediate to the CLI and SDM. The SMD provides granular configuration control by means of independent but closely coupled. One advantage of the SMD GUI is that it is possible to concurrently view all the ZBF functional groups. This is important because correct configuration mandates that the field of each functional group is correctly matched. The SDM also provides the ability to monitor both device status and firewall operation in real-time.

It can be concluded that, in the context of the HCI-S criteria, each method has relative strengths and weaknesses.

References

[1] Y. Bartal, A. Mayer, K. Nissim, and A. Wool, "Firmato: A novel firewall management toolkit," ACM Trans. Comput. Syst., vol.22, pp.381-420, 2004.

[2] T. Akker, Q.O. Snell, and M.J. Clement, "The YGuard access control model: set-based access control," Proceedings of the sixth ACM symposium on Access control models and technologies, 2001.

[3] E. Schultz, "The human factor in security," Computers & Security, vol.24, pp.425-426, 2005.

[4] J. Nielsen and R. Molich, "Heuristic evaluation of user interfaces," Proceedings of the SIGCHI conference on

Human factors in computing systems: Empowering people, 1990.

[5] J. Johnston, J.H.P. Eloff, and L. Labuschagne, "Security and human computer interfaces," Computers & Security, vol.22, pp.675-684, 2003.

[6] S.P. Maj, G. Murphy, and G. Kohli. "State models for internetworking technologies," IEEE Frontiers in Education, pp.F2G-10-15, 2004.

[7] S.P. Maj and D. Veal, "State Model Diagrams as a Pedagogical Tool: An International Evaluation," IEEE Transactions on Education, vol.50, pp.204-207, 2007.

[8] C. Nuangjamnong, S.P. Maj, and D. Veal, "Network security devices and protocols using state model diagrams," 5th Australian Information Security Management Conference, 2007.

[9] S.P. Maj, B. Tran, and D. Veal, "State Model Diagrams - a Systems Tool for Teaching Network Technologies and Network Management," International Joint Conferences on Computer, Information and Systems Sciences, and Engineering, 2007.

A/Prof S. P. Maj has been highly successful in linking applied research with curriculum development. In 2000 he was nominated ECU University Research Leader of the Year award. He was awarded an ECU Vice-Chancellor’s Excellence in Teaching Award in 2002, and again in 2009. He received a National Carrick Citation in 2006 for *“the development of world class curriculum and the design and implementation of associated world-class network teaching laboratories”*. He is the only Australian judge for the annual IEEE International Student Competition and was the first Australian reviewer for the American National Science Foundation (NSF) Courses, Curriculum and Laboratory Improvement (CCLI) program.

Dr. David Veal is a Senior Lecturer at Edith Cowan University. He is the manager of Cisco Network Academy Program at Edith Cowan University and be a unit coordinator of all Cisco network technology units. His research interests are in Graphical User Interface for the visually handicapped and also computer network modeling.

Woratat Makasiranondh received the B.Eng in Telecommunication Engineering from Suranaree University of Technology, and M.S. degrees in Computer Science from Rangsit University in 2001 and 2005, respectively. After working in the IT industry he became an academic member of Rangsit University. He is currently on study leave and undertaking his doctorate research at Edith Cowan University in the field of network technology education.