

CableHome™ Security MIB Specification

Superseded

CH-SP-MIB-SEC-I07-040806

Issued

Notice

This CableHome specification is a cooperative effort undertaken at the direction of Cable Television Laboratories, Inc. (CableLabs®) for the benefit of the cable industry. Neither CableLabs, nor any other entity participating in the creation of this document, is responsible for any liability of any nature whatsoever resulting from or arising out of use or reliance upon this document by any party. This document is furnished on an AS-IS basis and neither CableLabs, nor other participating entity, provides any representation or warranty, express or implied, regarding its accuracy, completeness, or fitness for a particular purpose.

© Copyright 2001 - 2004 Cable Television Laboratories, Inc.

All rights reserved.

Document Status Sheet

Document Control Number:	CH-SP-MIB-SEC-I07-040806		
Document Title:	CableHome™ Security MIB Specification		
Revision History:	I07 – August 6, 2004 I06 – April 9, 2004 I05 – January 29, 2004 I04 – August 1, 2003 I03 – April 11, 2003 I02 – September 20, 2002 I01 – April 5, 2002 D03 – March 21, 2002 D02 – January 31, 2002 D01 – January 8, 2002		
Date:	August 6, 2004		
Status:	Work in Progress	Draft	Issued
Distribution Restrictions:	Author Only	CL/Member	CL/CableHome/Vendor Public

Key to Document Status Codes:

Work in Progress	An incomplete document, designed to guide discussion and generate feedback, which may include several alternative requirements for consideration.
Draft	A document in specification format considered largely complete, but lacking review by Members and vendors. Drafts are susceptible to substantial change during the review process.
Issued	A stable document, which has undergone rigorous member and vendor review and is suitable for product design and development, cross-vendor interoperability, and for certification testing.
Closed	A static document, reviewed, tested, validated, and closed to further engineering change requests to the specification through CableLabs.

Trademarks:

DOCSIS®, eDOCSIS™, PacketCable™, CableHome™, CableOffice™, OpenCable™ and CableLabs® are trademarks of Cable Television Laboratories, Inc.

Contents

1	SCOPE	1
2	REFERENCES	1
	2.1 Normative References	1
	2.2 Reference Acquisition	1
3	ACRONYMS	1
4	REQUIREMENTS	2
5	ACKNOWLEDGEMENTS	30
	APPENDIX I REVISION HISTORY	31

This page left blank intentionally.

1 SCOPE

This specification describes CableHome Security (CH-SP-MIB) in terms of

2 REFERENCES

2.1 Normative References

In order to claim compliance with this specification, it is necessary to conform to the following standards and other works as indicated, in addition to the other requirements of this specification. Notwithstanding, intellectual property rights may be required to use or implement such normative references.

- [1] CableHome 1.0 Specification, CH-SP-CH1.0-I05-030801, August 1, 2003.
- [2] CableHome 1.1 Specification, CH-SP-CH1.1-I05-040806, August 6, 2004.
- [3] CableLabs® Definition MIB Specification, CL-SP-MIB-CLABDEF-I04-040804, August 4, 2004.

2.2 Reference Acquisition

CableLabs Specifications:

- Cable Television Laboratories, Inc., <http://www.cablelabs.com>

3 ACRONYMS

This specification uses the following acronyms:

CAP	CableHome Addressing Portal
CDC	CableHome DHCP Client (component of CDP)
CDP	CableHome DHCP Portal
CDS	CableHome DHCP Server (component of CDP)
CMP	CableHome Management Portal
CTP	CableHome Test Portal
DHCP	Dynamic Host Configuration Protocol
NAPT	Network Address and Port Translation
NAT	Network Address Translation
PS	Portal Services

4 REQUIREMENTS

The CableHome™ SEC MIB MUST be implemented as defined below.

```

CABH-SEC-MIB DEFINITIONS ::= BEGIN
IMPORTS
    MODULE-IDENTITY,
    Unsigned32,
    zeroDotZero,
    Counter32,
    OBJECT-TYPE                FROM SNMPv2-SMI    -- RFC2578

    DateAndTime,
    TruthValue,
    TimeStamp,
    RowStatus,
    VariablePointer            FROM SNMPv2-TC    -- RFC2579

    OBJECT-GROUP,
    MODULE-COMPLIANCE        FROM SNMPv2-CONF -- RFC2580
    InetPortNumber,
    InetAddress                FROM INET-ADDRESS-MIB --RFC3291

    SnmpAdminString          FROM SNMP-FRAMEWORK-MIB --RFC2571

    X509Certificate          FROM DOCS-BPI2-MIB

    ZeroBasedCounter32      FROM RMON2-MIB
    docsDevFilterIpEntry    FROM DOCS-CABLE-DEVICE-MIB
    InterfaceIndexOrZero    FROM IF-MIB

    clabProjCableHome      FROM CLAB-DEF-MIB;

cabhSecMib MODULE-IDENTITY
LAST-UPDATED    "200408060000Z" -- August 6, 2004
ORGANIZATION    "CableLabs Broadband Access Department"
CONTACT-INFO
    "Kevin Luehrs
     Postal: Cable Television Laboratories, Inc.
     858 Coal Creek Circle
     Louisville, Colorado 80027
     U.S.A.
     Phone: +1 303-661-9100
     Fax:   +1 303-661-9199
     E-mail: k.luehrs@cablelabs.com; mibs@cablelabs.com"
DESCRIPTION
    "This MIB module supplies the basic management
     objects for the Security Portal Services."
 ::= { clabProjCableHome 2 }

-- Textual conventions

cabhSecMibObjects OBJECT IDENTIFIER ::= { cabhSecMib 5 }
cabhSecFwObjects  OBJECT IDENTIFIER ::= { cabhSecMib 1 }
cabhSecFwBase     OBJECT IDENTIFIER ::= { cabhSecFwObjects 1 }
cabhSecFwLogCtl   OBJECT IDENTIFIER ::= { cabhSecFwObjects 2 }

cabhSecCertObjects OBJECT IDENTIFIER ::= { cabhSecMib 2 }
cabhSecKerbObjects OBJECT IDENTIFIER ::= { cabhSecMibObjects 3 }

```

```

cabhSecKerbBase      OBJECT IDENTIFIER ::= { cabhSecKerbObjects 1 }

cabhSec2FwObjects    OBJECT IDENTIFIER ::= { cabhSecMibObjects 4 }
cabhSec2FwBase       OBJECT IDENTIFIER ::= { cabhSec2FwObjects 1 }
cabhSec2FwEvent      OBJECT IDENTIFIER ::= { cabhSec2FwObjects 2 }
cabhSec2FwLog        OBJECT IDENTIFIER ::= { cabhSec2FwObjects 3 }
cabhSec2FwFilter     OBJECT IDENTIFIER ::= { cabhSec2FwObjects 4 }

--
--      CableHome 1.0 Base Firewall Functions
--

cabhSecFwPolicyFileEnable OBJECT-TYPE
    SYNTAX      INTEGER {
                    enable (1),
                    disable(2)
                }
    MAX-ACCESS   read-write
    STATUS       deprecated
    DESCRIPTION
        "This parameter indicates whether or not to enable
         the firewall functionality."
    DEFVAL { enable }
    ::= { cabhSecFwBase 1 }

cabhSecFwPolicyFileURL OBJECT-TYPE
    SYNTAX      SnmpAdminString
    MAX-ACCESS   read-write
    STATUS       deprecated
    DESCRIPTION
        "A policy rule set file download is triggered when the
         value used to SET this object is different than the value
         in the cabhSecFwPolicySuccessfulFileURL object."
    REFERENCE
        "CableHome 1.0 Specification, CH-SP-CH1.0-I05-030801,
         11.3.5.2 Firewall Rule Set Management Parameters."
    DEFVAL { "" }
    ::= { cabhSecFwBase 2 }

cabhSecFwPolicyFileHash OBJECT-TYPE
    SYNTAX      OCTET STRING (SIZE(0|20))
    MAX-ACCESS   read-write
    STATUS       deprecated
    DESCRIPTION
        "Hash of the contents of the rules set file,
         calculated and sent to the PS prior to sending
         the rules set file. For the SHA-1 authentication
         algorithm the length of the hash is 160 bits.
         This hash value is encoded in binary format."
    DEFVAL { 'h' }
    ::= { cabhSecFwBase 3 }

cabhSecFwPolicyFileOperStatus OBJECT-TYPE
    SYNTAX      INTEGER {
                    inProgress(1),
                    complete(2),
                    -- completeFromMgt(3), deprecated
                    failed(4)
                }
    MAX-ACCESS   read-only
    STATUS       deprecated
    DESCRIPTION
        "inProgress(1) indicates a firewall configuration

```

```

file download is underway.
complete (2) indicates the firewall configuration
file downloaded and configured successfully.
completeFromMgt(3) This state is deprecated.
failed(4) indicates the last attempted firewall
configuration file download or processing
failed ordinarily due to TFTP timeout."
 ::= { cabhSecFwBase 4 }

cabhSecFwPolicyFileCurrentVersion OBJECT-TYPE
SYNTAX      SnmpAdminString
MAX-ACCESS  read-only
STATUS      deprecated
DESCRIPTION
    "The rule set version currently operating in the
    PS device. This object should be in the syntax
    used by the individual vendor to identify software
    versions. Any PS element MUST return a string
    descriptive of the current rule set file load.
    If this is not applicable, this object MUST
    contain an empty string."
 ::= { cabhSecFwBase 5 }

cabhSecFwPolicySuccessfulFileURL OBJECT-TYPE
SYNTAX      SnmpAdminString
MAX-ACCESS  read-only
STATUS      deprecated
DESCRIPTION
    "Contains the location of the last successful downloaded
    policy rule set file in the format pointed in the
    reference. If a successful download has never occurred,
    this MIB object MUST report empty string."
REFERENCE
    "CableHome 1.0 Specification, CH-SP-CH1.0-I05-030801,
    11.3.5.2 Firewall Rule Set Management Parameters."
DEFVAL { "" }
 ::= { cabhSecFwBase 6 }

--
-- CableHome 1.0 Firewall Event MIBs
--

cabhSecFwEventType1Enable OBJECT-TYPE
SYNTAX      INTEGER {
                enable(1), -- log event
                disable(2) -- do not log event
            }
MAX-ACCESS  read-write
STATUS      deprecated
DESCRIPTION
    "This object enables or disables logging of type 1
    firewall event messages. Type 1 event messages report
    attempts from both private and public clients to
    traverse the firewall that violate the Security
    Policy."
DEFVAL { disable }
 ::= { cabhSecFwLogCtl 1 }

cabhSecFwEventType2Enable OBJECT-TYPE
SYNTAX      INTEGER {
                enable(1), -- log event
                disable(2) -- do not log event
            }

```

```
MAX-ACCESS read-write
STATUS deprecated
DESCRIPTION
    "This object enables or disables logging of
    type 2 firewall event messages. Type 2 event
    messages report identified Denial of Service
    attack attempts."
DEFVAL { disable }
 ::= { cabhSecFwLogCtl 2 }

cabhSecFwEventType3Enable OBJECT-TYPE
SYNTAX INTEGER {
    enable(1), -- log event
    disable(2) -- do not log event
}
MAX-ACCESS read-write
STATUS deprecated
DESCRIPTION
    "Enables or disables logging of type 3 firewall
    event messages. Type 3 event messages report
    changes made to the following firewall management
    parameters: cabhSecFwPolicyFileURL,
    cabhSecFwPolicyFileCurrentVersion,
    cabhSecFwPolicyFileEnable"
DEFVAL { disable }
 ::= { cabhSecFwLogCtl 3 }

cabhSecFwEventAttackAlertThreshold OBJECT-TYPE
SYNTAX INTEGER (0..65535)
MAX-ACCESS read-write
STATUS deprecated
DESCRIPTION
    "If the number of type 1 or 2 hacker attacks
    exceeds this threshold in the period define
    by cabhSecFwEventAttackAlertPeriod, a firewall
    message event MUST be logged with priority
    level 4."
DEFVAL { 65535 }
 ::= { cabhSecFwLogCtl 4 }

cabhSecFwEventAttackAlertPeriod OBJECT-TYPE
SYNTAX INTEGER (0..65535)
MAX-ACCESS read-write
STATUS deprecated
DESCRIPTION
    "Indicates the period to be used (in hours) for
    the cabhSecFwEventAttackAlertThreshold. This MIB
    variable should always keep track of the last x
    hours of events meaning that if the variable is
    set to track events for 10 hours then when the
    11th hour is reached, the 1st hour of events is
    deleted from the tracking log. A default value
    is set to zero, meaning zero time, so that this
    MIB variable will not track any events unless
    configured."
DEFVAL { 0 }
 ::= { cabhSecFwLogCtl 5 }

--
-- CableHome PS device certificate
--

cabhSecCertPsCert OBJECT-TYPE
```

```

SYNTAX      X509Certificate
MAX-ACCESS  read-only
STATUS      current
DESCRIPTION
    "The X509 DER-encoded PS certificate."
 ::= { cabhSecCertObjects 1 }

--
-- CableHome 1.1 Firewall Management MIBs
--

cabhSec2FwEnable OBJECT-TYPE
    SYNTAX      INTEGER {
                    enabled(1),
                    disabled(2)
                }
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
        "This parameter indicates whether to enable or disable the
         firewall."
    DEFVAL { enabled }
    ::= { cabhSec2FwBase 1 }

cabhSec2FwPolicyFileURL OBJECT-TYPE
    SYNTAX      SnmpAdminString
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
        "A policy rule set file download is triggered when the
         value used to SET this object is different than the value
         in the cabhSec2FwPolicySuccessfulFileURL object."
    REFERENCE
        "CableHome 1.1 Specification, CH-SP-CH1.1-I05-040806,
         11.6.4.8.1 Firewall Rule Set Management MIB Objects."
    DEFVAL { "" }
    ::= { cabhSec2FwBase 2 }

cabhSec2FwPolicyFileHash OBJECT-TYPE
    SYNTAX      OCTET STRING (SIZE(0|20))
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
        "Hash of the contents of the firewall
         configuration file. For the SHA-1 authentication
         algorithm the length of the hash is 160 bits.
         This hash value is encoded in binary format."
    DEFVAL { 'h' }
    ::= { cabhSec2FwBase 3 }

cabhSec2FwPolicyFileOperStatus OBJECT-TYPE
    SYNTAX      INTEGER {
                    inProgress(1),
                    complete(2),
                    failed(3)
                }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "InProgress(1) indicates a firewall configuration
         file download is underway. Complete(2) indicates
         the firewall configuration file was downloaded
         and processed successfully. Failed(3) indicates

```

```
        that the last attempted firewall configuration
        file download or processing failed."
 ::= { cabhSec2FwBase 4 }

cabhSec2FwPolicyFileCurrentVersion OBJECT-TYPE
    SYNTAX      SnmpAdminString
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
        "A label set by the cable operator that can be
        used to track various versions of configured
        rulesets. Once the label is set and configured
        rules are changed, it may not accurately reflect
        the version of configured rules running on the box.
        If this object has never been configured, it MUST
        contain an empty string."
    DEFVAL { "" }
 ::= { cabhSec2FwBase 5 }

cabhSec2FwClearPreviousRuleset OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
        "If set to 'true', the PS MUST clear all entries in the
        docsDevFilterIpTable. Reading this value always returns
        false."
    REFERENCE
        "CableHome specification - Security section"
    DEFVAL { false }
 ::= { cabhSec2FwBase 6 }

cabhSec2FwPolicySelection OBJECT-TYPE
    SYNTAX      INTEGER {
        factoryDefault(1),
        configuredRulesetBoth(2),
        factoryDefaultAndConfiguredRulesetBoth(3),
        configuredRulesetDocsDevFilterIpTable(4),
        configuredRulesetCabhSec2FwLocalFilterIpTable (5),
        factoryDefaultAndDocsDevFilterIpTable (6),
        factoryDefaultAndCabhSec2FwLocalFilterIpTable (7)
    }
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
        "This object allows for selection of the filtering policy
        as defined by the following options:

        factoryDefault (1) The firewall filters against the Factory
        Default Ruleset in the cabhSec2FwFactoryDefaultFilterTable.

        configuredRulesetBoth (2) The firewall filters against the
        Configured Ruleset defined by both the
        docsDevFilterIpTable and the cabhSec2FwLocalFilterIpTable.

        factoryDefaultAndConfiguredRulesetBoth (3) The firewall
        filters against the CableHome specified Factory Default
        Ruleset in the cabhSec2FwFactoryDefaultFilterTable and
        the Configured Ruleset in the docsDevFilterIpTable and
        the cabhSec2FwLocalFilterIpTable.

        configuredRulesetDocsDevFilterIpTable(4) The firewall
        filters against the Configured Ruleset defined by the
```

docsDevFilterIpTable.

configuredRulesetCabhSec2FwLocalFilterIpTable (5) The firewall filters against the Configured Ruleset defined by the cabhSec2FwLocalFilterIpTable.

factoryDefaultAndDocsDevFilterIpTable (6) The firewall filters against the Factory Default Ruleset and the Configured Ruleset defined by the DocsDevFilterIpTable.

factoryDefaultAndCabhSec2FwLocalFilterIpTable (7) The firewall filters against the Factory Default Ruleset and the Configured Ruleset defined by the cabhSec2FwLocalFilterIpTable."

REFERENCE

"CableHome specification - Security section."

DEFVAL { factoryDefault }
::= { cabhSec2FwBase 7 }

cabhSec2FwEventSetToFactory OBJECT-TYPE

SYNTAX TruthValue
MAX-ACCESS read-write
STATUS current

DESCRIPTION

"If set to 'true', entries in cabhSec2FwEventControlEntry are set to their default values.
Reading this value always returns false."

DEFVAL { false }
::= { cabhSec2FwBase 8 }

cabhSec2FwEventLastSetToFactory OBJECT-TYPE

SYNTAX TimeStamp
MAX-ACCESS read-only
STATUS current

DESCRIPTION

"The value of sysUpTime when cabhSec2FwEventSetToFactory was last set to true. Zero if never reset."

::= { cabhSec2FwBase 9 }

cabhSec2FwPolicySuccessfulFileURL OBJECT-TYPE

SYNTAX SnmpAdminString
MAX-ACCESS read-only
STATUS current

DESCRIPTION

"Contains the location of the last successful downloaded policy rule set file in the format pointed in the reference. If a successful download has not yet occurred, this MIB object should report empty string."

REFERENCE

"CableHome 1.1 Specification, CH-SP-CH1.1-I05-040806, 11.6.4.8.1 Firewall Rule Set Management MIB Objects."

DEFVAL { "" }
::= { cabhSec2FwBase 10 }

cabhSec2FwConfiguredRulesetPriority OBJECT-TYPE

SYNTAX INTEGER {
docsDevFilterIpTable (1),
cabhSec2FwLocalFilterIpTable (2)
}

MAX-ACCESS read-write
STATUS current

DESCRIPTION

"This object defines which Configured Ruleset filter rule

has priority when a conflict exists between a filter rule in the docsDevFilterIpTable and a filter rule in the cabhSec2FwLocalFilterIpTable as indicated by the following options:

docsDevFilterIpTable (1) - indicates that filter rules in the docsDevFilterIpTable have priority over any conflicting filters that may exist in the cabhSec2FwLocalFilterIpTable.

cabhSec2FwLocalFilterIpTable (2) - indicates that filter rules in the cabhSec2FwLocalFilterIpTable have priority over any conflicting filters that may exist in the docsDevFilterIpTable."

REFERENCE

"CableHome specification - Security section."

```
DEFVAL { cabhSec2FwLocalFilterIpTable }
::= { cabhSec2FwBase 11 }
```

cabhSec2FwClearLocalRuleset OBJECT-TYPE

```
SYNTAX      TruthValue
```

```
MAX-ACCESS  read-write
```

```
STATUS      current
```

DESCRIPTION

"If set to 'true', the PS MUST clear all entries in the cabhSec2FwLocalFilterIpTable. Reading this value always returns false."

REFERENCE

"CableHome specification - Security section"

```
DEFVAL { false }
```

```
::= { cabhSec2FwBase 12 }
```

```
-- ++++++
```

```
--
```

```
-- CableHome 1.1 Firewall Event MIBS
```

```
--
```

cabhSec2FwEventControlTable OBJECT-TYPE

```
SYNTAX      SEQUENCE OF CabhSec2FwEventControlEntry
```

```
MAX-ACCESS  not-accessible
```

```
STATUS      current
```

DESCRIPTION

"This table controls the reporting of the Firewall Attacks events"

```
::= { cabhSec2FwEvent 1 }
```

cabhSec2FwEventControlEntry OBJECT-TYPE

```
SYNTAX      CabhSec2FwEventControlEntry
```

```
MAX-ACCESS  not-accessible
```

```
STATUS      current
```

DESCRIPTION

"Allows configuration of the reporting mechanisms for a particular type of attack."

```
INDEX { cabhSec2FwEventType }
```

```
::= { cabhSec2FwEventControlTable 1 }
```

```
CabhSec2FwEventControlEntry ::= SEQUENCE {
```

```
  cabhSec2FwEventType      INTEGER,
```

```
  cabhSec2FwEventEnable    INTEGER,
```

```
  cabhSec2FwEventThreshold Unsigned32,
```

```
  cabhSec2FwEventInterval  Unsigned32,
```

```

cabhSec2FwEventCount      ZeroBasedCounter32,
cabhSec2FwEventLogReset   TruthValue,
cabhSec2FwEventLogLastReset  TimeStamp
}

cabhSec2FwEventType OBJECT-TYPE
    SYNTAX      INTEGER      {
        type1(1),
        type2(2),
        type3(3),
        type4(4),
        type5(5),
        type6(6)
    }
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION
        "Classification of the different types of
        attacks.
        Type 1 logs all attempts from both LAN and WAN
        clients to traverse the Firewall that violate the
        Security Policy.
        Type 2 logs identified Denial of Service attack
        attempts.
        Type 3 logs all changes made to the
        cabhSec2FwPolicyFileURL,
        cabhSec2FwPolicyFileCurrentVersion or
        cabhSec2FwPolicyFileEnable objects.
        Type 4 logs all failed attempts to modify
        cabhSec2FwPolicyFileURL and
        cabhSec2FwPolicyFileEnable objects.
        Type 5 logs allowed inbound packets from the WAN.
        Type 6 logs allowed outbound packets from the
        LAN."
    ::= { cabhSec2FwEventControlEntry 1 }

cabhSec2FwEventEnable OBJECT-TYPE
    SYNTAX      INTEGER      {
        enabled(1),
        disabled(2)
    }
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION
        "Enables or disables counting and logging of
        firewall events by type as assigned by
        cabhSec2FwEventType."
    DEFVAL { disabled }
    ::= { cabhSec2FwEventControlEntry 2 }

cabhSec2FwEventThreshold OBJECT-TYPE
    SYNTAX      Unsigned32 (0..65535)
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION
        "Number of attacks to count before sending the
        appropriate event by type as assigned by
        cabhSec2FwEventType."
    DEFVAL { 0 }
    ::= { cabhSec2FwEventControlEntry 3 }

cabhSec2FwEventInterval OBJECT-TYPE
    SYNTAX      Unsigned32 (0..744)

```

```

UNITS          "hours"
MAX-ACCESS    read-write
STATUS        current
DESCRIPTION
    "Indicates the time interval in hours to count and log
    occurrences of a firewall event type as assigned in
    cabhSec2FwEventType. If this MIB has a value of zero
    then there is no interval assigned and the PS will not
    count or log events."
DEFVAL { 0 }
 ::= { cabhSec2FwEventControlEntry 4 }

cabhSec2FwEventCount OBJECT-TYPE
    SYNTAX      ZeroBasedCounter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Indicates the current count up to the
        cabhSec2FwEventThreshold value by type as
        assigned by cabhSec2FwEventType."
    ::= { cabhSec2FwEventControlEntry 5 }

cabhSec2FwEventLogReset OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
        "Setting this object to true clears the log table
        for the specified event type. Reading this object
        always returns false."
    DEFVAL { false }
    ::= { cabhSec2FwEventControlEntry 6 }

cabhSec2FwEventLogLastReset OBJECT-TYPE
    SYNTAX      TimeStamp
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The value of sysUpTime when cabhSec2FwEventLogReset was
        last set to true. Zero if never reset."
    ::= { cabhSec2FwEventControlEntry 7 }

--
-- CableHome 1.1 Firewall Log Tables
--

cabhSec2FwLogTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF CabhSec2FwLogEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "Contains a log of packet information as related
        to events enabled by the cable operator. The types
        are defined in the CableHome 1.1 specification and
        require various objects to be included in the log.
        The following is a description for what is
        expected in the log for each type Type 1, Type 2,
        Type 5 and Type 6 table MUST include
        cabhSec2FwEventType, cabhSec2FwEventPriority,
        cabhSec2FwEventId, cabhSec2FwLogTime,
        cabhSec2FwIpProtocol, cabhSec2FwIpSourceAddr,
        cabhSec2FwIpDestAddr, cabhSec2FwIpSourcePort,
        cabhSec2FwIpDestPort, cabhSec2Fw,

```

```

        cabhSec2FwReplayCount. The other values not used
        by Types 1, 2, 5 and 6 are default values. Type 3
        and Type 4 MUST include cabhSec2FwEventType,
        cabhSec2FwEventPriority, cabhSec2FwEventId,
        cabhSec2FwLogTime, cabhSec2FwIpSourceAddr,
        cabhSec2FwLogMIBPointer. The other values not used
        by type 3 and 4 are default values. When applicable,
        Type 1, Type 5, and Type 6 MUST also include
        cabhSec2FwLogMatchingFilterTableName,
        cabhSec2FwLogMatchingFilterTableIndex,
        cabhSec2FwLogMatchingFilterDescr."
 ::= { cabhSec2FwLog 1 }

cabhSec2FwLogEntry OBJECT-TYPE
    SYNTAX      CabhSec2FwLogEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "Each entry contains the log of firewall events"
    INDEX {cabhSec2FwLogIndex}
 ::= { cabhSec2FwLogTable 1 }

CabhSec2FwLogEntry ::= SEQUENCE {
    cabhSec2FwLogIndex          Unsigned32,
    cabhSec2FwLogEventType     INTEGER,
    cabhSec2FwLogEventPriority  INTEGER,
    cabhSec2FwLogEventId       Unsigned32,
    cabhSec2FwLogTime           DateAndTime,
    cabhSec2FwLogIpProtocol     Unsigned32,
    cabhSec2FwLogIpSourceAddr   InetAddress,
    cabhSec2FwLogIpDestAddr     InetAddress,
    cabhSec2FwLogIpSourcePort   InetPortNumber,
    cabhSec2FwLogIpDestPort     InetPortNumber,
    cabhSec2FwLogMessageType    Unsigned32,
    cabhSec2FwLogReplayCount    Unsigned32,
    cabhSec2FwLogMIBPointer     VariablePointer,
    cabhSec2FwLogMatchingFilterTableName  INTEGER,
    cabhSec2FwLogMatchingFilterTableIndex Unsigned32,
    cabhSec2FwLogMatchingFilterDescr     SnmpAdminString
}

cabhSec2FwLogIndex OBJECT-TYPE
    SYNTAX      Unsigned32 (1..2147483647)
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A sequence number for the specific events
        under a cabhSec2FwEventType."
 ::= { cabhSec2FwLogEntry 1 }

cabhSec2FwLogEventType OBJECT-TYPE
    SYNTAX      INTEGER      {
        type1(1),
        type2(2),
        type3(3),
        type4(4),
        type5(5),
        type6(6)
    }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Classification of the different types of

```

```

attacks.
Type 1 logs all attempts from both LAN and WAN
clients to traverse the Firewall that violate
the Security Policy.
Type 2 logs identified Denial of Service attack
attempts.
Type 3 logs all changes made to the
cabhSec2FwPolicyFileURL,
cabhSec2FwPolicyFileCurrentVersion or
cabhSec2FwPolicyFileEnable objects.
Type 4 logs all failed attempts to modify
cabhSec2FwPolicyFileURL and
cabhSec2FwPolicyFileEnable objects.
Type 5 logs allowed inbound packets from the WAN.
Type 6 logs allowed outbound packets from the
LAN."
 ::= { cabhSec2FwLogEntry 2 }

cabhSec2FwLogEventPriority OBJECT-TYPE
    SYNTAX      INTEGER      {
        emergency(1),
        alert(2),
        critical(3),
        error(4),
        warning(5),
        notice(6),
        information(7),
        debug(8)
    }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The priority level of this event as defined
        by CableHome Specification. If a priority is
        not assigned in the CableHome specification for
        a particular event then the vendor or cable
        operator may assign priorities. These are
        ordered from most serious (emergency) to least
        serious (debug)."
```

```

 ::= { cabhSec2FwLogEntry 3 }

cabhSec2FwLogEventId OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The assigned event ID."
 ::= { cabhSec2FwLogEntry 4 }

cabhSec2FwLogTime OBJECT-TYPE
    SYNTAX      DateAndTime
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The time that this entry was created by the PS."
 ::= { cabhSec2FwLogEntry 5 }

cabhSec2FwLogIpProtocol OBJECT-TYPE
    SYNTAX      Unsigned32 (0..256)
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The IP Protocol."
```

```

 ::= { cabhSec2FwLogEntry 6 }

cabhSec2FwLogIpSourceAddr OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The Source IP Address of the packet logged."
 ::= { cabhSec2FwLogEntry 7 }

cabhSec2FwLogIpDestAddr OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The Destination IP Address of the packet logged."
 ::= { cabhSec2FwLogEntry 8 }

cabhSec2FwLogIpSourcePort OBJECT-TYPE
    SYNTAX      InetPortNumber
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The Source IP Port of the packet logged."
 ::= { cabhSec2FwLogEntry 9 }

cabhSec2FwLogIpDestPort OBJECT-TYPE
    SYNTAX      InetPortNumber
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The Source IP Port of the packet logged."
 ::= { cabhSec2FwLogEntry 10 }

cabhSec2FwLogMessageType OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The ICMP defined types."
 ::= { cabhSec2FwLogEntry 11}

cabhSec2FwLogReplayCount OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The number of identical attack packets that
         were seen by the firewall based on
         cabhSec2FwLogIpProtocol, cabhSec2FwLogIpSourceAddr,
         cabhSec2FwLogIpDestAddr, cabhSec2FwLogIpSourcePort,
         cabhSec2FwLogIpDestPort and cabhSec2FwLogMessageType."
    DEFVAL { 0 }
 ::= { cabhSec2FwLogEntry 12 }

cabhSec2FwLogMIBPointer OBJECT-TYPE
    SYNTAX      VariablePointer
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Identifies if the cabhSec2FwPolicyFileURL or the
         cabhSec2FwEnable MIB object changed or an attempt
         was made to change it."

```

```

DEFVAL { zeroDotZero }
 ::= { cabhSec2FwLogEntry 13 }

cabhSec2FwLogMatchingFilterTableName OBJECT-TYPE
    SYNTAX      INTEGER      {
        cabhSec2FwFactoryDefaultFilterTable(1),
        docsDevFilterIpTable(2),
        cabhSec2FwLocalFilterIpTable(3),
        none(4)
    }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "When applicable, cabhSec2FwLogMatchingFilterTableName
        indicates the filter table name containing the last filter
        rule matched that caused the event to be generated."
    DEFVAL { none }
    ::= { cabhSec2FwLogEntry 14 }

cabhSec2FwLogMatchingFilterTableIndex OBJECT-TYPE
    SYNTAX      Unsigned32 (0..2147483647)
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "When applicable, cabhSec2FwLogMatchingFilterTableIndex
        indicates the filter table index if the last filter
        rule matched that caused the event to be generated. If
        the value is 0, the event was not caused by a filter
        rule match. "
    DEFVAL { 0 }
    ::= { cabhSec2FwLogEntry 15 }

cabhSec2FwLogMatchingFilterDescr OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE(0..32))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "When applicable, cabhSec2FwLogMatchingFilterDescr
        contains the description value found in the
        cabhSec2FwFilterScheduleDesc MIB object or the
        cabhSec2FwLocalFilterIpDesc MIB object of the last
        filter rule matched that caused the event to be
        generated."
    DEFVAL { "" }
    ::= { cabhSec2FwLogEntry 16 }

-- =====
--
-- CableHome 1.1 PS IP Filter Scheduling Table
--
-- The cabhSec2FwFilterScheduleTable contains the firewall
-- policy identification and links that policy as defined
-- in RFC 2669 to specific time of day restrictions.
--
-- =====

cabhSec2FwFilterScheduleTable OBJECT-TYPE
    SYNTAX SEQUENCE OF CabhSec2FwFilterScheduleEntry
    MAX-ACCESS not-accessible
    STATUS      current
    DESCRIPTION
        "Extends the filtering matching parameters of
        docsDevFilterIpTable defined in RFC 2669 for CableHome

```

```

        Residential Gateways to include time day intervals and days
        of the week."
 ::= { cabhSec2FwFilter 1 }

cabhSec2FwFilterScheduleEntry OBJECT-TYPE
    SYNTAX      CabhSec2FwFilterScheduleEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "Extended values for entries of docsDevFilterIpTable.
        If the PS has not acquire ToD the entire
        docsDevFilterIpEntry rule set is ignored.
        Note: A filter time period may include two days
        (e.g from 10 PM to 4 AM). A filter time period that
        includes two days is identified by the absolute value
        of the cabhSec2FwFilterScheduleEndTime being less than the
        absolute value of the cabhSec2FwFilterScheduleStartTime.
        The cabhSec2FwFilterScheduleDOW setting and the
        cabhSec2FwFilterScheduleStartTime value indicate what day
        and time the filter becomes active. The
        cabhSec2FwFilterScheduleEndTime indicates when the filter
        becomes inactive on the second day. The maximum filter
        time period that includes two days is 24 hours.
        If cabhSec2FwFilterScheduleStartTime is less than or
        equal to the cabhSec2FwFilterScheduleEndTime the time
        period of the filter falls in the same day."
    AUGMENTS { docsDevFilterIpEntry }
 ::= { cabhSec2FwFilterScheduleTable 1 }

CabhSec2FwFilterScheduleEntry ::= SEQUENCE {
    cabhSec2FwFilterScheduleStartTime    Unsigned32,
    cabhSec2FwFilterScheduleEndTime     Unsigned32,
    cabhSec2FwFilterScheduleDOW         BITS,
    cabhSec2FwFilterScheduleDescr       SnmpAdminString
}

cabhSec2FwFilterScheduleStartTime OBJECT-TYPE
    SYNTAX      Unsigned32 (0..2359)
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
        "The start time for matching the filter ruleset in the
        specified days indicated in cabhSec2FwFilterScheduleDOW.
        Time is represented in Military Time, e.g., 8:30 AM is
        represented as 830 and 11:45 PM as 2345. An attempt to set
        this object to an invalid military time value, e.g., 1182,
        returns 'wrongValue' error."
    DEFVAL { 0 }
 ::= { cabhSec2FwFilterScheduleEntry 1 }

cabhSec2FwFilterScheduleEndTime OBJECT-TYPE
    SYNTAX      Unsigned32 (0..2359)
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
        "The end time for matching the filter rule for the
        days indicated in cabhSec2FwFilterScheduleDOW. The filter
        rule associated with this end time MUST not be disabled
        until the minute following the time indicated by this
        MIB object. If the time period is for two days,
        identified by cabhSec2FwFilterScheduleEndTime being
        less than cabhSec2FwFilterScheduleStartTime, then

```

```

        the cabhSec2FwFilterScheduleDOW settings
        do not apply to this MIB object.
        Time is represented in the same manner as in
        cabhSec2FwFilterScheduleStartTime. An attempt to set
        this object to an invalid military time value, e.g., 1182,
        returns 'wrongValue' error."
DEFVAL { 2359 }
 ::= { cabhSec2FwFilterScheduleEntry 2 }

cabhSec2FwFilterScheduleDOW OBJECT-TYPE
    SYNTAX BITS {
        sunday(0),
        monday(1),
        tuesday(2),
        wednesday(3),
        thursday(4),
        friday(5),
        saturday(6)
    }
    MAX-ACCESS read-create
    STATUS current
    DESCRIPTION
        "If the day of week bit associated with the PS given day
        is '1', this object criteria matches."
    DEFVAL { 'fe'h } -- 1111110 Sun-Sat
    ::= { cabhSec2FwFilterScheduleEntry 3 }

cabhSec2FwFilterScheduleDescr OBJECT-TYPE
    SYNTAX SnmpAdminString (SIZE(0..32))
    MAX-ACCESS read-create
    STATUS current
    DESCRIPTION
        "A filter rule description configured by the
        cable operator or subscriber."
    DEFVAL { "" }
    ::= { cabhSec2FwFilterScheduleEntry 4 }

-- =====
--
-- CableHome 1.1 PS Firewall Factory Default Filter Table
--
-- The cabhSec2FwFactoryDefaultFilterTable contains the
-- firewall factory default ruleset in a read only table as
-- defined by the CableLabs CableHome 1.1 Specification.
--
-- =====

cabhSec2FwFactoryDefaultFilterTable OBJECT-TYPE
    SYNTAX SEQUENCE OF CabhSec2FwFactoryDefaultFilterEntry
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "Contains the firewall factory default ruleset as
        defined by the CableLabs CableHome 1.1 Specification."
    ::= { cabhSec2FwFilter 2 }

cabhSec2FwFactoryDefaultFilterEntry OBJECT-TYPE
    SYNTAX CabhSec2FwFactoryDefaultFilterEntry
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "Contains the firewall factory default ruleset."
    INDEX {cabhSec2FwFactoryDefaultFilterIndex }

```

```

 ::= { cabhSec2FwFactoryDefaultFilterTable 1 }

CabhSec2FwFactoryDefaultFilterEntry ::= SEQUENCE {
  cabhSec2FwFactoryDefaultFilterIndex      Unsigned32,
  cabhSec2FwFactoryDefaultFilterControl    INTEGER,
  cabhSec2FwFactoryDefaultFilterIfIndex    InterfaceIndexOrZero,
  cabhSec2FwFactoryDefaultFilterDirection  INTEGER,
  cabhSec2FwFactoryDefaultFilterSaddr      InetAddress,
  cabhSec2FwFactoryDefaultFilterSmask      InetAddress,
  cabhSec2FwFactoryDefaultFilterDaddr      InetAddress,
  cabhSec2FwFactoryDefaultFilterDmask      InetAddress,
  cabhSec2FwFactoryDefaultFilterProtocol   Unsigned32,
  cabhSec2FwFactoryDefaultFilterSourcePortLow  Unsigned32,
  cabhSec2FwFactoryDefaultFilterSourcePortHigh Unsigned32,
  cabhSec2FwFactoryDefaultFilterDestPortLow   Unsigned32,
  cabhSec2FwFactoryDefaultFilterDestPortHigh Unsigned32,
  cabhSec2FwFactoryDefaultFilterContinue     TruthValue
}

cabhSec2FwFactoryDefaultFilterIndex OBJECT-TYPE
  SYNTAX      Unsigned32 (1..2147483647)
  MAX-ACCESS  not-accessible
  STATUS      current
  DESCRIPTION
    "Index used to order the application of filters.
     The filter with the lowest index is always applied
     first."
 ::= { cabhSec2FwFactoryDefaultFilterEntry 1 }

cabhSec2FwFactoryDefaultFilterControl OBJECT-TYPE
  SYNTAX      INTEGER {
                deny(1),
                allow(2)
              }
  MAX-ACCESS  read-only
  STATUS      current
  DESCRIPTION
    "If set to deny(1), all packets matching this filter
     will be discarded. If set to allow(2), all
     packets matching this filter will be accepted.
     The cabhSec2FwFactoryDefaultFilterContinue object is
     Set to true, and therefore the PS MUST continue to
     scan the table for other matches to apply the match
     with the highest cabhSec2FwFactoryDefaultFilterIndex
     value."
 ::= { cabhSec2FwFactoryDefaultFilterEntry 2 }

cabhSec2FwFactoryDefaultFilterIfIndex OBJECT-TYPE
  SYNTAX      InterfaceIndexOrZero
  MAX-ACCESS  read-only
  STATUS      current
  DESCRIPTION
    "The index number assigned to this object MUST
     match to the IfIndex numbering assigned in the
     ifTable from the Interfaces Group MIB [RFC 2863],
     and as specified in CH 1.1 Spec, Table 6-16
     Numbering Interfaces in the ifTable. If the value
     is zero, the filter applies to all interfaces.
     This object MUST be specified to create a row in
     this table."
 ::= { cabhSec2FwFactoryDefaultFilterEntry 3 }

cabhSec2FwFactoryDefaultFilterDirection OBJECT-TYPE

```

```

SYNTAX      INTEGER {
                inbound(1),
                outbound(2),
                both(3)
            }
MAX-ACCESS  read-only
STATUS      current
DESCRIPTION
    "This value represents direction in relationship
    to the assigned
    cabhSec2FwFactoryDefaultFilterIfIndex
    in this particular rule, meaning that the PS
    MUST represent traffic direction as follows:
    inbound(1)traffic, outbound(2) traffic, or
    both(3)inbound and outbound traffic."
 ::= { cabhSec2FwFactoryDefaultFilterEntry 4 }

cabhSec2FwFactoryDefaultFilterSaddr OBJECT-TYPE
SYNTAX      InetAddress
MAX-ACCESS  read-only
STATUS      current
DESCRIPTION
    "The source IP address, or portion thereof, that is
    to be matched for this filter. The source address
    is first masked (and'ed) against
    cabhSec2FwFactoryDefaultFilterSmask
    before being compared to this value. A value of 0
    for this object and 0 for the mask matches all IP
    addresses."
DEFVAL { '00000000'h }
 ::= { cabhSec2FwFactoryDefaultFilterEntry 5 }

cabhSec2FwFactoryDefaultFilterSmask OBJECT-TYPE
SYNTAX      InetAddress
MAX-ACCESS  read-only
STATUS      current
DESCRIPTION
    "A bit mask that is to be applied to the source
    address prior to matching. This mask is not
    necessarily the same as a subnet mask, but 1's
    bits must be leftmost and contiguous."
DEFVAL { '00000000'h }
 ::= { cabhSec2FwFactoryDefaultFilterEntry 6 }

cabhSec2FwFactoryDefaultFilterDaddr OBJECT-TYPE
SYNTAX      InetAddress
MAX-ACCESS  read-only
STATUS      current
DESCRIPTION
    "The destination IP address, or portion thereof, that
    is to be matched for this filter. The destination
    address is first masked (and'ed) against
    cabhSec2FwFactoryDefaultFilterDmask
    before being compared to this value. A value of 0
    for this object and 0 for the mask matches all
    IP addresses."
DEFVAL { '00000000'h }
 ::= { cabhSec2FwFactoryDefaultFilterEntry 7 }

cabhSec2FwFactoryDefaultFilterDmask OBJECT-TYPE
SYNTAX      InetAddress
MAX-ACCESS  read-only
STATUS      current

```

```

DESCRIPTION
    "A bit mask that is to be applied to the destination
    address prior to matching. This mask is not necessarily
    the same as a subnet mask, but 1's bits must be leftmost
    and contiguous."
DEFVAL { '00000000'h }
::= { cabhSec2FwFactoryDefaultFilterEntry 8 }

cabhSec2FwFactoryDefaultFilterProtocol OBJECT-TYPE
    SYNTAX      Unsigned32 (0..65535)
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The protocol value that is to be matched. For example:
        icmp is 1, tcp is 6, udp is 17. A value of 65535 matches
        ANY protocol."
    DEFVAL { 65535 }
    ::= { cabhSec2FwFactoryDefaultFilterEntry 9 }

cabhSec2FwFactoryDefaultFilterSourcePortLow OBJECT-TYPE
    SYNTAX      Unsigned32 (0..65535)
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "If cabhSec2FwFactoryDefaultFilterProtocol is udp
        or tcp, this is the inclusive lower bound of the
        transport-layer source port range that is to be
        matched, otherwise it is ignored during matching."
    DEFVAL { 0 }
    ::= { cabhSec2FwFactoryDefaultFilterEntry 10 }

cabhSec2FwFactoryDefaultFilterSourcePortHigh OBJECT-TYPE
    SYNTAX      Unsigned32 (0..65535)
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "If cabhSec2FwFactoryDefaultFilterProtocol is
        udp or tcp, this is the inclusive upper bound
        of the transport-layer source port range that
        is to be matched, otherwise it is ignored
        during matching."
    DEFVAL { 65535 }
    ::= { cabhSec2FwFactoryDefaultFilterEntry 11 }

cabhSec2FwFactoryDefaultFilterDestPortLow OBJECT-TYPE
    SYNTAX      Unsigned32 (0..65535)
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "If cabhSec2FwFactoryDefaultFilterProtocol is
        udp or tcp, this is the inclusive lower bound
        of the transport-layer destination port range
        that is to be matched, otherwise it is ignored
        during matching."
    DEFVAL { 0 }
    ::= { cabhSec2FwFactoryDefaultFilterEntry 12 }

cabhSec2FwFactoryDefaultFilterDestPortHigh OBJECT-TYPE
    SYNTAX      Unsigned32 (0..65535)
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "If cabhSec2FwFactoryDefaultFilterProtocol is

```

```

        udp or tcp, this is the inclusive upper bound
        of the transport-layer destination port range
        that is to be matched, otherwise it is ignored
        during matching."
DEFVAL { 65535 }
 ::= { cabhSec2FwFactoryDefaultFilterEntry 13 }

cabhSec2FwFactoryDefaultFilterContinue OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "This value is always set to true so the PS MUST continue
        scanning and applying rules."
    DEFVAL { true }
    ::= { cabhSec2FwFactoryDefaultFilterEntry 14 }

-- =====
--
-- CableHome 1.1 PS Firewall Local Filter Table
--
-- The cabhSec2FwLocalFilterIpTable can be configured to contain
-- a filtering Ruleset for the PS firewall. It can be used to
-- support subscriber specific or local filtering rules that
-- are separate from general filtering rules that may be
-- be configured in the docsDevFilterIpTable.
-- =====

cabhSec2FwLocalFilterIpTable OBJECT-TYPE
    SYNTAX SEQUENCE OF CabhSec2FwLocalFilterIpEntry
    MAX-ACCESS not-accessible
    STATUS      current
    DESCRIPTION
        "Contains a configured filtering Ruleset for the
        PS firewall."
    ::= { cabhSec2FwFilter 3 }

cabhSec2FwLocalFilterIpEntry OBJECT-TYPE
    SYNTAX      CabhSec2FwLocalFilterIpEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "Contains a configured filter rule for the PS
        firewall.

        If the PS has not acquired ToD, entries that do not have
        default time settings are ignored.

        Note, that a filter time period may include two days
        (e.g from 10 PM to 4 AM). A filter time period that
        includes two days is identified by the absolute value of
        the cabhSec2FwLocalFilterIpEndTime being less than the
        absolute value of the cabhSec2FwLocalFilterIpStartTime.
        The cabhSec2FwLocalFilterIpDOW setting and the
        cabhSec2FwLocalFilterIpStartTime value indicate what day
        and time the filter becomes active. The
        cabhSec2FwLocalFilterIpEndTime indicates when the filter
        becomes inactive on the second day. The maximum filter time
        period that includes two days is 24 hours.

        If cabhSec2FwLocalFilterIpStartTime is less than or equal
        to the cabhSec2FwLocalFilterIpEndTime the time period
        of the filter falls in the same day."

```

```

INDEX { cabhSec2FwLocalFilterIpIndex }
 ::= { cabhSec2FwLocalFilterIpTable 1 }

CabhSec2FwLocalFilterIpEntry ::= SEQUENCE {
  cabhSec2FwLocalFilterIpIndex      Unsigned32,
  cabhSec2FwLocalFilterIpStatus     RowStatus,
  cabhSec2FwLocalFilterIpControl    INTEGER,
  cabhSec2FwLocalFilterIpIfIndex    InterfaceIndexOrZero,
  cabhSec2FwLocalFilterIpDirection  INTEGER,
  cabhSec2FwLocalFilterIpSaddr      InetAddress,
  cabhSec2FwLocalFilterIpSmask      InetAddress,
  cabhSec2FwLocalFilterIpDaddr      InetAddress,
  cabhSec2FwLocalFilterIpDmask      InetAddress,
  cabhSec2FwLocalFilterIpProtocol   Unsigned32,
  cabhSec2FwLocalFilterIpSourcePortLow  Unsigned32,
  cabhSec2FwLocalFilterIpSourcePortHigh Unsigned32,
  cabhSec2FwLocalFilterIpDestPortLow   Unsigned32,
  cabhSec2FwLocalFilterIpDestPortHigh  Unsigned32,
  cabhSec2FwLocalFilterIpMatches      Counter32,
  cabhSec2FwLocalFilterIpContinue     TruthValue,
  cabhSec2FwLocalFilterIpStartTime    Unsigned32,
  cabhSec2FwLocalFilterIpEndTime     Unsigned32,
  cabhSec2FwLocalFilterIpDOW         BITS,
  cabhSec2FwLocalFilterIpDescr       SnmpAdminString
}

cabhSec2FwLocalFilterIpIndex OBJECT-TYPE
  SYNTAX      Unsigned32 (1..2147483647)
  MAX-ACCESS  not-accessible
  STATUS      current
  DESCRIPTION
    "Index used to order the application of filters.
     The filter with the lowest index is always applied
     first."
  ::= { cabhSec2FwLocalFilterIpEntry 1 }

cabhSec2FwLocalFilterIpStatus OBJECT-TYPE
  SYNTAX      RowStatus
  MAX-ACCESS  read-create
  STATUS      current
  DESCRIPTION
    "Controls and reflects the status of rows in this
     table. Creation of the
     rows may be done via either create-and-wait or
     create-and-go, but the filter is not applied until this
     object is set to (or changes to) active. There is no
     restriction in changing any object in a row while this
     object is set to active."
  ::= { cabhSec2FwLocalFilterIpEntry 2 }

cabhSec2FwLocalFilterIpControl OBJECT-TYPE
  SYNTAX      INTEGER {
                deny(1),
                allow(2)
              }
  MAX-ACCESS  read-create
  STATUS      current
  DESCRIPTION
    "If set to deny(1), all packets matching this filter
     will be discarded. If set to allow(2), all
     packets matching this filter will be accepted.
     The cabhSec2FwLocalFilterIpContinue object is

```

```

        Set to true, and therefore the PS MUST continue to
        scan the table for other matches to apply the match
        with the highest cabhSec2FwLocalFilterIpIndex
        value."
 ::= { cabhSec2FwLocalFilterIpEntry 3 }

cabhSec2FwLocalFilterIpIfIndex OBJECT-TYPE
    SYNTAX      InterfaceIndexOrZero
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
        "The index number assigned to this object MUST
        match to the IfIndex numbering assigned in the
        ifTable from the Interfaces Group MIB [RFC 2863],
        and as specified in CH 1.1 Spec, Table 6-16
        Numbering Interfaces in the ifTable."
    DEFVAL { 255 }
 ::= { cabhSec2FwLocalFilterIpEntry 4 }

cabhSec2FwLocalFilterIpDirection OBJECT-TYPE
    SYNTAX      INTEGER {
                inbound(1),
                outbound(2),
                both(3)
                }
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
        "This value represents direction in relationship
        to the assigned cabhSec2FwLocalFilterIpIfIndex
        in this particular rule, meaning that the PS
        MUST represent traffic direction as follows:
        inbound(1)traffic, outbound(2) traffic, or
        both(3)inbound and outbound traffic."
 ::= { cabhSec2FwLocalFilterIpEntry 5 }

cabhSec2FwLocalFilterIpSaddr OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
        "The source IP address, or portion thereof, that is
        to be matched for this filter. The source address
        is first masked (and'ed) against
        cabhSec2FwLocalFilterIpSmask before being compared to this
        value. A value of 0 for this object and 0 for the mask
        matches all IP addresses."
    DEFVAL { '00000000'h }
 ::= { cabhSec2FwLocalFilterIpEntry 6 }

cabhSec2FwLocalFilterIpSmask OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
        "A bit mask that is to be applied to the source
        address prior to matching. This mask is not
        necessarily the same as a subnet mask, but 1's
        bits must be leftmost and contiguous."
    DEFVAL { '00000000'h }
 ::= { cabhSec2FwLocalFilterIpEntry 7 }

cabhSec2FwLocalFilterIpDaddr OBJECT-TYPE
```

```

SYNTAX      InetAddress
MAX-ACCESS  read-create
STATUS      current
DESCRIPTION
    "The destination IP address, or portion thereof, that
    is to be matched for this filter. The destination
    address is first masked (and'ed) against
    cabhSec2FwLocalFilterIpDmask
    before being compared to this value. A value of 0
    for this object and 0 for the mask matches all
    IP addresses."
DEFVAL { '00000000'h }
::= { cabhSec2FwLocalFilterIpEntry 8 }

cabhSec2FwLocalFilterIpDmask OBJECT-TYPE
SYNTAX      InetAddress
MAX-ACCESS  read-create
STATUS      current
DESCRIPTION
    "A bit mask that is to be applied to the destination
    address prior to matching. This mask is not necessarily
    the same as a subnet mask, but 1's bits must be leftmost
    and contiguous."
DEFVAL { '00000000'h }
::= { cabhSec2FwLocalFilterIpEntry 9 }

cabhSec2FwLocalFilterIpProtocol OBJECT-TYPE
SYNTAX      Unsigned32 (0..65535)
MAX-ACCESS  read-create
STATUS      current
DESCRIPTION
    "The protocol value that is to be matched. For example:
    icmp is 1, tcp is 6, udp is 17. A value of 65535 matches
    ANY protocol."
DEFVAL { 65535 }
::= { cabhSec2FwLocalFilterIpEntry 10 }

cabhSec2FwLocalFilterIpSourcePortLow OBJECT-TYPE
SYNTAX      Unsigned32 (0..65535)
MAX-ACCESS  read-create
STATUS      current
DESCRIPTION
    "If cabhSec2FwLocalFilterIpProtocol is udp
    or tcp, this is the inclusive lower bound of the
    transport-layer source port range that is to be
    matched, otherwise it is ignored during matching."
DEFVAL { 0 }
::= { cabhSec2FwLocalFilterIpEntry 11 }

cabhSec2FwLocalFilterIpSourcePortHigh OBJECT-TYPE
SYNTAX      Unsigned32 (0..65535)
MAX-ACCESS  read-create
STATUS      current
DESCRIPTION
    "If cabhSec2FwLocalFilterIpProtocol is
    udp or tcp, this is the inclusive upper bound
    of the transport-layer source port range that
    is to be matched, otherwise it is ignored
    during matching."
DEFVAL { 65535 }
::= { cabhSec2FwLocalFilterIpEntry 12 }

cabhSec2FwLocalFilterIpDestPortLow OBJECT-TYPE

```

```
SYNTAX      Unsigned32 (0..65535)
MAX-ACCESS  read-create
STATUS      current
DESCRIPTION
    "If cabhSec2FwLocalFilterIpProtocol is
    udp or tcp, this is the inclusive lower bound
    of the transport-layer destination port range
    that is to be matched, otherwise it is ignored
    during matching."
DEFVAL { 0 }
 ::= { cabhSec2FwLocalFilterIpEntry 13 }

cabhSec2FwLocalFilterIpDestPortHigh OBJECT-TYPE
SYNTAX      Unsigned32 (0..65535)
MAX-ACCESS  read-create
STATUS      current
DESCRIPTION
    "If cabhSec2FwLocalFilterIpProtocol is
    udp or tcp, this is the inclusive upper bound
    of the transport-layer destination port range
    that is to be matched, otherwise it is ignored
    during matching."
DEFVAL { 65535 }
 ::= { cabhSec2FwLocalFilterIpEntry 14 }

cabhSec2FwLocalFilterIpMatches OBJECT-TYPE
SYNTAX      Counter32
MAX-ACCESS  read-only
STATUS      current
DESCRIPTION
    "Counts the number of times this filter was matched.
    This object is initialized to 0 at boot, or at row
    creation, and is reset only upon reboot."
 ::= { cabhSec2FwLocalFilterIpEntry 15 }

cabhSec2FwLocalFilterIpContinue OBJECT-TYPE
SYNTAX      TruthValue
MAX-ACCESS  read-only
STATUS      current
DESCRIPTION
    "This value is always set to true so the PS MUST continue
    scanning and applying rules."
DEFVAL { true }
 ::= { cabhSec2FwLocalFilterIpEntry 16 }

cabhSec2FwLocalFilterIpStartTime OBJECT-TYPE
SYNTAX      Unsigned32 (0..2359)
MAX-ACCESS  read-create
STATUS      current
DESCRIPTION
    "The start time for matching the filter ruleset in the
    specified days indicated in cabhSec2FwLocalFilterIpDOW.
    Time is represented in Military Time, e.g., 8:30 AM is
    represented as 830 and 11:45 PM as 2345. An attempt to set
    this object to an invalid military time value, e.g., 1182,
    returns 'wrongValue' error."
DEFVAL { 0 }
 ::= { cabhSec2FwLocalFilterIpEntry 17 }

cabhSec2FwLocalFilterIpEndTime OBJECT-TYPE
SYNTAX      Unsigned32 (0..2359)
MAX-ACCESS  read-create
STATUS      current
```

```

DESCRIPTION
    "The end time for matching the filter ruleset for the
    days indicated in cabhSec2FwLocalFilterIpDOW. The filter
    rule associated with this end time MUST not be disabled
    until the minute following the time indicated by this
    MIB object. If the time period is for two days, identified
    by cabhSec2FwLocalFilterIpEndTime being less than
    cabhSec2FwLocalFilterIpStartTime, then the
    cabhSec2FwLocalFilterIpDOW settings do not apply to this
    MIB object. Time is represented in the same manner as in
    cabhSec2FwLocalFilterIpStartTime. An attempt to set
    this object to an invalid military time value, e.g., 1182,
    returns 'wrongValue' error."
DEFVAL { 2359 }
 ::= { cabhSec2FwLocalFilterIpEntry 18 }

cabhSec2FwLocalFilterIpDOW OBJECT-TYPE
    SYNTAX BITS {
        sunday(0),
        monday(1),
        tuesday(2),
        wednesday(3),
        thursday(4),
        friday(5),
        saturday(6)
    }
    MAX-ACCESS read-create
    STATUS current
    DESCRIPTION
        "If the day of week bit associated with the PS given day
        is '1', this object criteria matches."
    DEFVAL { 'fe'h } -- 11111110 Sun-Sat
    ::= { cabhSec2FwLocalFilterIpEntry 19 }

cabhSec2FwLocalFilterIpDescr OBJECT-TYPE
    SYNTAX SnmpAdminString (SIZE(0..32))
    MAX-ACCESS read-create
    STATUS current
    DESCRIPTION
        "A filter rule description configured by the
        cable operator or subscriber."
    DEFVAL { "" }
    ::= { cabhSec2FwLocalFilterIpEntry 20 }

--
-- Kerberos MIBs
--

cabhSecKerbPKINITGracePeriod OBJECT-TYPE
    SYNTAX Unsigned32 (15..600)
    UNITS "minutes"
    MAX-ACCESS read-write
    STATUS current
    DESCRIPTION
        "The PKINIT Grace Period is needed by the PS
        to know when it should start retrying to get
        a new ticket. The PS MUST obtain a new Kerberos
        ticket (with a PKINIT exchange) this many minutes
        before the old ticket expires."
    DEFVAL { 30 }
    ::= { cabhSecKerbBase 1}

cabhSecKerbTGSGracePeriod OBJECT-TYPE

```

```

SYNTAX      Unsigned32 (1..600)
UNITS       "minutes"
MAX-ACCESS  read-write
STATUS      current
DESCRIPTION
    "The TGS Grace Period is needed by the PS to
    know when it should start retrying to get a new
    ticket. The PS MUST obtain a new Kerberos ticket
    (with a TGS Request) this many minutes before the
    old ticket expires."
DEFVAL { 10 }
 ::= { cabhSecKerbBase 2 }

cabhSecKerbUnsolicitedKeyMaxTimeout OBJECT-TYPE
SYNTAX      Unsigned32 (15..600)
UNITS       "seconds"
MAX-ACCESS  read-write
STATUS      current
DESCRIPTION
    "This timeout applies to PS initiated AP-REQ/REP
    key management exchange with NMS. The maximum
    timeout is the value which may not be exceeded in
    the exponential backoff algorithm."
DEFVAL { 600 }
 ::= { cabhSecKerbBase 3 }

cabhSecKerbUnsolicitedKeyMaxRetries OBJECT-TYPE
SYNTAX      Unsigned32 (1..32)
MAX-ACCESS  read-write
STATUS      current
DESCRIPTION
    "The number of retries the PS is allowed for
    AP-REQ/REP key management exchange initiation
    with the NMS. This is the maximum number of
    retries before the PS gives up attempting to
    establish an SNMPv3 security association
    with NMS."
DEFVAL { 8 }
 ::= { cabhSecKerbBase 4 }

cabhSecNotification OBJECT IDENTIFIER ::= { cabhSecMib 3 }
cabhSecConformance OBJECT IDENTIFIER ::= { cabhSecMib 4 }
cabhSecCompliances OBJECT IDENTIFIER ::= { cabhSecConformance 1 }
cabhSecGroups OBJECT IDENTIFIER ::= { cabhSecConformance 2 }

--
-- Notification Group for future extension
--

-- compliance statements

cabhSecCompliance MODULE-COMPLIANCE
STATUS      deprecated
DESCRIPTION
    "The compliance statement for CableHome Security."
MODULE     --cabhSecMib

-- unconditionally mandatory groups

MANDATORY-GROUPS {
    cabhSecCertGroup,
    cabhSecKerbGroup
}

```

```

-- conditional mandatory groups

GROUP cabhSecGroup
DESCRIPTION
    "This group is implemented only for CH 1.0 gateways."
 ::= { cabhSecCompliances 1 }

cabhSec2Compliance MODULE-COMPLIANCE
STATUS      current
DESCRIPTION
    "The compliance statement for CableHome 1.1 Security."
MODULE     --cabhSecMib

-- unconditionally mandatory groups

MANDATORY-GROUPS {
    cabhSecCertGroup,
    cabhSecKerbGroup,
    cabhSec2Group
}
 ::= { cabhSecCompliances 2 }

cabhSecGroup OBJECT-GROUP
OBJECTS {
    cabhSecFwPolicyFileEnable,
    cabhSecFwPolicyFileURL,
    cabhSecFwPolicyFileHash,
    cabhSecFwPolicyFileOperStatus,
    cabhSecFwPolicyFileCurrentVersion,
    cabhSecFwPolicySuccessfulFileURL,
    cabhSecFwEventType1Enable,
    cabhSecFwEventType2Enable,
    cabhSecFwEventType3Enable,
    cabhSecFwEventAttackAlertThreshold,
    cabhSecFwEventAttackAlertPeriod
}
STATUS      deprecated
DESCRIPTION
    "Group of objects in CableHome 1.0 Firewall MIB."
 ::= { cabhSecGroups 1 }

cabhSecCertGroup OBJECT-GROUP
OBJECTS {
    cabhSecCertPsCert
}
STATUS      current
DESCRIPTION
    "Group of objects in CableHome gateway for PS
    Certificate."
 ::= { cabhSecGroups 2 }

cabhSecKerbGroup OBJECT-GROUP
OBJECTS {
    cabhSecKerbPKINITGracePeriod,
    cabhSecKerbTGSGracePeriod,
    cabhSecKerbUnsolicitedKeyMaxTimeout,
    cabhSecKerbUnsolicitedKeyMaxRetries
}
STATUS      current
DESCRIPTION
    "Group of objects in CableHome gateway for Kerberos."
 ::= { cabhSecGroups 3 }

```

```
cabhSec2Group OBJECT-GROUP
  OBJECTS {
    cabhSec2FwEnable,
    cabhSec2FwPolicyFileURL,
    cabhSec2FwPolicyFileHash,
    cabhSec2FwPolicyFileOperStatus,
    cabhSec2FwPolicyFileCurrentVersion,
    cabhSec2FwClearPreviousRuleset,
    cabhSec2FwPolicySelection,
    cabhSec2FwEventSetToFactory,
    cabhSec2FwEventLastSetToFactory,
    cabhSec2FwPolicySuccessfulFileURL,
    cabhSec2FwEventEnable,
    cabhSec2FwEventThreshold,
    cabhSec2FwEventInterval,
    cabhSec2FwEventCount,
    cabhSec2FwEventLogReset,
    cabhSec2FwEventLogLastReset,
    cabhSec2FwLogEventType,
    cabhSec2FwLogEventPriority,
    cabhSec2FwLogEventId,
    cabhSec2FwLogTime,
    cabhSec2FwLogIpProtocol,
    cabhSec2FwLogIpSourceAddr,
    cabhSec2FwLogIpDestAddr,
    cabhSec2FwLogIpSourcePort,
    cabhSec2FwLogIpDestPort,
    cabhSec2FwLogMessageType,
    cabhSec2FwLogReplayCount,
    cabhSec2FwLogMIBPointer,
    cabhSec2FwFilterScheduleStartTime,
    cabhSec2FwFilterScheduleEndTime,
    cabhSec2FwFilterScheduleDOW,
    cabhSec2FwFactoryDefaultFilterControl,
    cabhSec2FwFactoryDefaultFilterIfIndex,
    cabhSec2FwFactoryDefaultFilterDirection,
    cabhSec2FwFactoryDefaultFilterSaddr,
    cabhSec2FwFactoryDefaultFilterSmask,
    cabhSec2FwFactoryDefaultFilterDaddr,
    cabhSec2FwFactoryDefaultFilterDmask,
    cabhSec2FwFactoryDefaultFilterProtocol,
    cabhSec2FwFactoryDefaultFilterSourcePortLow,
    cabhSec2FwFactoryDefaultFilterSourcePortHigh,
    cabhSec2FwFactoryDefaultFilterDestPortLow,
    cabhSec2FwFactoryDefaultFilterDestPortHigh,
    cabhSec2FwFactoryDefaultFilterContinue
  }
  STATUS          current
  DESCRIPTION
    "Group of objects in CableHome 1.1 Firewall MIB."
  ::= { cabhSecGroups 4 }

END
```

5 ACKNOWLEDGEMENTS

Nancy Davoust of YAS Broadband Ventures
Eduardo Cardona of CableLabs
Jim Hinsey, Broadcom Visiting Engineer
John Bevilacqua of YAS Broadband Ventures

Appendix I Revision History

The following Engineering Change Notices were incorporated into CH-SP-MIB-SEC-I02-020920:

ECN Number	ECN Date	Summary
CH1-N-02024	8/15/02	<p>Correct formatting of Description field for object <i>cabhSecFwPolicyFileURL</i>.</p> <p>Clarify the description of the encoding of the SHA-1 hash in the Description field of object <i>cabhSecFwPolicyFileHash</i>.</p> <p>Correct spelling error in the Description field for object <i>cabhSecFwPolicyFileCurrentVersion</i>.</p> <p>Add definition of ‘type 1’, ‘type 2’, and ‘type 3’ messages in the Description fields for objects <i>cabhSecFwEventType1Enable</i>, <i>cabhSecFwEventType2Enable</i>, and <i>cabhSecFwEventType3Enable</i>.</p> <p>Clarify the use of object <i>cabhSecFwEventAttackAlertPeriod</i>.</p> <p>Fix the Reference field for object <i>cabhSecCertPsCert</i>.</p> <p>Correct the MANDATORY GROUPS specification.</p>

The following Engineering Change Notices were incorporated into CH-SP-MIB-SEC-I03-030411:

ECN Number	ECN Date	Summary
CH1-N-02072	2/6/03	<p>Change MIB object <i>cabhSecFwPolicyFileOperStatus</i> description. The current description is not indicating clearly which state it should return when the TFTP download is completed successfully.</p>

The following Engineering Change Notices were incorporated into CH-SP-MIB-SEC-I04-030801:

ECN Number	ECN Date	Summary
CH1-N-03006	4/17/03	<p>Update the CableHome Security MIB for CableHome 1.1 Functionality.</p>
CH-MIB-N-03036	7/3/03	<p>Update Security MIB to support firewall URL MIB changes.</p>

The following Engineering Change Notices were incorporated into CH-SP-MIB-SEC-I05-040129:

ECN Number	ECN Date	Summary
MIB-SEC-N-03.0082-5	12/4/2003	Update SEC MIBs to support increment feature change

The following Engineering Change Notices were incorporated into CH-SP-MIB-SEC-I06-040409:

ECN Number	ECN Date	Summary
MIB-SEC-N-04.0121-2	3/11/2004	FW filter rule time change

The following Engineering Change Notices were incorporated into CH-SP-MIB-SEC-I07-040806:

ECN Number	ECN Date	Summary
MIB-SEC-N-04.0132-2	7/8/04	Local FW Filter MIB addition and related changes