SMTP

Module Overview

- SMTP operations
- Email components
- Email forwarding

SMTP Overview

- Text-based standard (RFC 5321) for electronic mail communication
  - Client-Server architecture
    - Server
      - Listens on TCP port 25
    - Client
      - Mail User Agent (MUA) or Mail Transfer Agent (MTA)
  - Command-Response behavior
    - SMTP Conversation is initiated by a client
      - Commands & data
    - Server replies with a Code & text
  - Only used to „push” emails

Email Components

- Envelope
  - Used for email delivery
- Data
  - Header
  - Body/Message
- Common Header Fields
  - From, Date, To, Subject, CC

Email Forwarding

- Emails are delivered based on the destination domain
  - E.g. kate@cisco.com -> cisco.com
  - Requires working DNS
    - A domain should be configured with at least one „MX” record
      - Priority + FQDN
    - Multiple entries can exist for redundancy and/or load balancing
      - Lower number -> higher priority
    - The domain „A” record acts as a fallback

SMTP Commands

- For details go to RFC 5321
  - HELO/EHLO
  - MAIL FROM
    - Envelope Sender address
  - RCPT TO
    - Envelope Recipient address
  - DATA
  - STARTTLS
  - QUIT

SMTP Response Codes

- Use a 3-digit format (xyz)
  - 2yz/3yz -> success
  - 4yz/5yz -> error
- Common Codes
  - 250 (command is accepted)
  - 354 (OK but waiting for more data)
  - 421 (temporary rejection - connection level)
  - 452 (temporary rejection - recipient level)
  - 550 (fatal error)

Sample Conversation

```
1 220 esa.example.com ESMTP
2 HELO sdomain.com
3 250 esa.example.com
4 MAIL FROM: <piotr@sdomain.com>
5 250 sender <piotr@sdomain.com> ok
6 RCPT TO: <piotr@example.com>
7 250 recipient <piotr@example.com> ok
8 DATA
9 354 go ahead
10 Subject: Example Message
11
12 Text of an example message.
13 .
14 250 ok: Message xxxx accepted
15 QUIT
16 221 esa.example.com
```

ESA Overview

Module Overview

- Introduction to ESA
- Platforms types
- Interfaces & design

What is ESA?

- Advanced email filtering solution
  - Protection, security & control
  - Not a SMTP server

- Key Features
  - Email traffic & content control
  - Malware protection
  - Data Loss Prevention
  - Authentication & Encryption

ESA Platform Types

- Physical
  - C1xx (SMB), C3xx (Medium Office) & C6xx (Large Enterprise)
    - Disk Space, CPU & RAM
- Virtual
  - ESXi & UCS
    - C000v, C100v, C300v & C600v

ESA Ports & Design

- ESA includes two or more ports labeled as „Data”
  - Used for data & management traffic
  - Management (M1) port is available on most platforms
    - Same as data ports
- ESA is commonly deployed behind a firewall
  - Internet Edge (DMZ)
  - Needs certain firewall rules

ESA Initialization

Module Overview

- Basic ESA Setup
- CLI
- Listener

ESA Initialization

- Basic ESA setup is performed using Setup Wizard
  - First-time login (GUI) or **systemsetup** (CLI)
  - Physical appliances are preconfigured with a default IP 192.168.42.42 (/24)
    - ESA listens on TCP port 80 (HTTP) and 443 (HTTPS)

- CLI is an alternative for management settings
  - SSH
  - Console

ESA Command Line

- ESA runs on AsyncOS
  - Partially similar to the IOS equivalent
    - Command completion (Tab), process termination (CTRL+C), etc.
  - Many commands use the “Interactive Mode”
  - Config changes must be approved (**commit**) to take effect

Useful CLI Syntax

- Basic Setup
  - **etherconfig**
    - L1/L2 interface settings – duplex, speed, VLANs & more
  - **interfaceconfig**
    - L3 interface settings – IP address, mask, etc.
  - **routeconfig**
    - Static IP routes
    - To add a default route use **setgateway** instead
  - **ntpconfig**
    - NTP Server(s)

Useful CLI Syntax

- DNS
  - **dnsconfig**
    - DNS Server(s)
  - **dnsflush**
    - Clear cache
  - **nslookup, dig**
    - Testing
      - **nslookup cisco.com**
      - **dig @1.2.3.4 cisco.com**

Useful CLI Syntax

- Verification & Troubleshooting
  - **ping, traceroute, telnet**
    - Basic connectivity
  - **tail**
    - ESA logs
  - **packetcapture**
    - TCP Dump
  - **mailconfig**
    - Test email

Useful CLI Syntax

- Verification & Troubleshooting
  - **status [detail]**
    - RAM/CPU/Disk utilization, uptime, licensing
    - Counters (soft/hard bounces, rejected recipients, etc.)
  - **hoststatus**
  - **topin**
  - **trace**
  - **diagnostic -> network -> smtpping**
    - Remote SMTP server testing

The Listener

- SMTP deamon required to process email traffic
  - Controls connection setup & major ESA features
    - Host Access Table (HAT), Recipient Access Table (RAT)
  - A number of Listeners used depends on the organization
    - One Listener may be hard to manage & offers less bandwidth
    - Two Listeners (Public & Private) make an alternative
      - Two interfaces are preferred but one is enough
  - Blackhole Listener can be created for troubleshooting

Email Pipeline

Module Overview

- Email Handling

Email Processing

- ESA processes emails in three phases
  - SMTP Server
  - WorkQueue
  - SMTP Client

Email Pipeline

SMTP SERVER	WORKQUEUE	SMTP CLIENT
HAT	LDAP RCPT Accept	Encryption
Received Header	Masquerading	Virtual Gateways
Default Domain	LDAP Routing	Delivery Limits
Domain Map	Message Filters	Received: Header
RAT	Anti-SPAM	Domain-Based Limits
Alias Table	Anti-Virus	Domain-Based Routing
LDAP RCPT Accept	AMP	Global Unsubscribe
SMTP Call-Ahead	Graymail	S/MIME Encryption
DKIM/SPF Verification	Content Filters	DKIM Signing
DMARC Verification	Outbreak Filters	Bounce Profiles
S/MIME Verification	DLP	Message Delivery

Access Tables

Module Overview

- Initial flow processing
- HAT
- RAT

Initial Flow Processing

- ESA starts flow processing at the TCP level
  - Double DNS lookup
    - Reverse (connecting IP address) & Forward (returned FQDN)
      - If any lookup fails or results don't match, Sender is deemed unverified
  - SenderBase Reputation Score (SBRS) lookup
    - Sender's IP i checked against the SenderBase
- The SBRS, IP & FQDN (optional) information is then used by HAT

Host Access Table (HAT)

- A set of rules controlling email Senders
  - Who can connect & how
  - Rules consist of Sender Groups (conditions) & Mail Flow Policies (results)
    - Top-down first-match processing
      - Sender Group conditions are processed as logical OR
    - The Default Rule allows everyone (ALL) to connect (ACCEPTED)

HAT Elements

- Sender Group
  - SBRS
  - IP address, IP range
  - FQDN, domain
    - Only if the Sender is verified (double DNS lookup match)
  - Unverified Senders
- Mail Flow Policy
  - Controls SMTP conversation
    - Message & recipient limits, SPAM & virus protection, encryption & more
  - Classifies messages as incoming or outgoing

HAT Elements

- Mail Flow Policy Actions
  - Continue
  - Accept
    - Connection is accepted & treated as incoming
      - Email acceptance is limited according to RAT
  - Relay
    - Connection is accepted & treated as outgoing
      - RAT is not used
  - TCP Refuse
  - Reject

Recipient Access Table (RAT)

- Destination-based email filtering mechanism
  - Emails can be accepted or rejected based on the recipient address (RCPT TO)
    - No processing & forwarding messages sent to invalid recipients
      - Saves resources, no bounce messages
    - Stops ESA from acting as an Open Relay

- RAT checks don't apply to Private Listeners

RAT Elements

- RAT supports few types of entries
  - Domain or partial domain
    - E.g. *domain.com* or *.domain.com*
  - User
    - E.g. *user@domain.com* or *user@*
  - IP address
  - LDAP lookups may be enabled for additional verification
- The Default RAT Rule rejects all emails
  - Most/all custom rules will be configured with “Accept”
    - Top-down first-match processing

Next Steps

- ESA's authentication and/or encryption services are optional
  - Successful HAT & RAT check normally allows Senders to continue with DATA

SMTP SERVER	WORKQUEUE
HAT	LDAP RCPT Accept
Received Header	Masquerading
Default Domain	LDAP Routing
Domain Map	Message Filters
RAT	Anti-SPAM
Alias Table	Anti-Virus
LDAP RCPT Accept	AMP
SMTP Call-Ahead	Graymail
DKIM/SPF Verification	Content Filters
DMARC Verification	Outbreak Filters
S/MIME Verification	DLP

Introduction to Policies

Module Overview

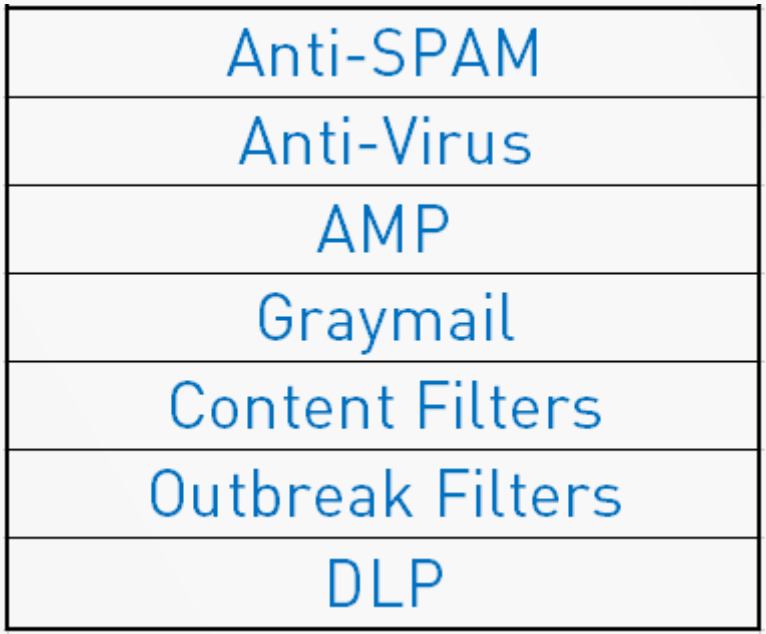
- ESA Policies Overview
- Mail Policies

ESA Policies

- Used to satisfy different security needs of users and/or groups

- Configuration Steps
  - Policy Engine activation
  - Mail Policy definition
    - Incoming
      - HAT “ACCEPT”
    - Outgoing
      - HAT “RELAY”
  - Policy settings configuration

Policy Engines



Mail Policies

- Evaluated based on message address(es)
  - Sender
    - Envelope Sender (MAIL FROM)
    - Message Header (“From:”, “Reply-To:”)
  - Recipient
    - Envelope Recipient (RCPT TO)
      - Final address only
    - Messages sent to more than one recipient may be Splintered
      - Occurs if all recipients don’t match the same Policy
- The Policy Table is evaluated from the top to the bottom

ESA Policies Part I

Module Overview

- Anti-SPAM
- Graymail
- Anti-Virus

Anti-SPAM

- ESA uses a special scoring system to detect unwanted messages
  - Relies on SenderBase & 100,000+ message attributes
  - Score & thresholds classify a message as legitimate, or positive/suspected SPAM

- Configuration
  - Engine activation
    - **Security Services -> IronPort Anti-Spam**
  - Settings & actions
    - **Mail Policies**

Graymail

- Email traffic users signed up for
  - Newsletters, mailing list subscriptions, social media notifications, etc.
  - Graymails can be not only filtered, but also securely “turned off”
    - Unsubscribe Service
  - Requires working Anti-SPAM

- Configuration
  - Engine activation
    - **Security Services -> Detection and Safe Unsubscribe**
  - Policy actions
    - **Mail Policies**

Anti-Virus

- ESA includes two local AV scanning engines : Sophos & McAfee
  - Multi-layer scans are possible
    - First McAfee, then Sophos

- Configuration
  - Engine activation
    - **Security Services -> McAfee**
    - **Security Services -> Sophos**
  - Scanning actions
    - **Mail Policies**

ESA Policies Part II

Module Overview

- Outbreak Filters
- Content Filters

Outbreak Filters

- Responsible for real-time detection of new emerging threats
  - Viral
    - Virus attachments (never seen before)
  - Non-viral
    - Messages with links to external malware/phishing/scam websites
- Outbreak Filters don’t impose any final action on the message
  - Delay
  - Redirect
  - Modify

Outbreak Filters

- Outbreak Filters are composed of two types of rules
  - Outbreak
    - Global data
    - Frequent updates (“real time”)
  - Adaptive
    - Signature-based local scanning

- The rules are scanned by Context Adaptive Scanning Engine (CASE)
  - Message score is mapped to a Threat Level
    - 0 (no risk) through 5 (extreme risk)
  - Action are ordered based on configured Policy thresholds

Outbreak Filters

- Pre-requisites
  - Anti-SPAM
    - Non-viral threats
  - Anti-Virus (optional)

- Configuration
  - Engine activation
    - **Security Services -> Outbreak Filters**
  - Settings & tuning
    - **Mail Policies**

Content Filters

- Advanced scanning of incoming and/or outgoing messages
  - Filtering, alteration, encryption, notifications & more
  - Similar to Message Filters with some exceptions
    - GUI support
      - **Mail Policies -> Incoming Content Filters**
      - **Mail Policies -> Outgoing Content Filters**
    - Processed after Anti-SPAM/Virus, AMP & Graymail

Content Filters

- Configuration Steps
  - Supporting Features (optional)
  - Filter Condition(s) (optional)
    - Otherwise affects all messages matching the associated Mail Policy
  - Filter Action(s)
    - Non-final
      - BCC, Quarantine, Strip Attachment & more
    - Final
      - Drop, Bounce, Skip, Encrypt & S/MIME Sign/Encrypt
  - Action Variables (optional)

Message Filters

Module Overview

- Feature overview
- Configuration syntax & examples

Message Filters

- Powerful filtering engine used for advanced email handling
  - Dropping, bouncing, archiving, altering & more
  - Kick in before Security Policies
    - Apply to the entire mail flow (no Splintering)
  - More flexible than Content Filters
    - Conditions & actions

- Available only through CLI
  - **filters**
    - Strict programming-language–like syntax
      - Use notepad & fallback to GUI (Content Filters) if in trouble

Message Filters

- A Message Filter consists of a Name, Rule(s) & Action(s)
  - Name
    - Ends with ":"
  - Rule(s)
    - If (*condition1* AND/OR *condition2* …) { *action* }
      - "else" is optional
  - Action(s)
    - Final
      - drop(); bounce(); encrypt(); & skip-filters();
    - Non-final
      - notify(); bcc(); log(); drop-attachments-by-name(); & more

Message Filters

- Example #1

```
SPM:
if (subject == “^SPAM.*”) AND (rcpt-to == “john@example.com”) {
    notify(“admin@example.com”);
    drop();
}
```

Message Filters

- Example #2

```
DSPOOF:
if (mail-from == “example\.com$”) {
    drop();
}
else {
    no-op();
}
```